PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-124941
(43)Date of publication of application : 26.04.2002

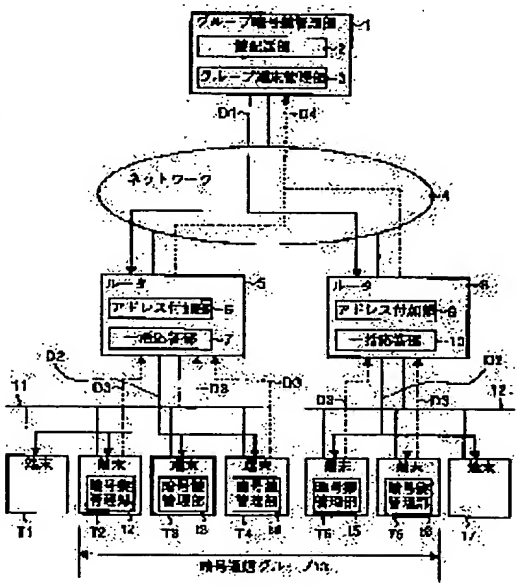
(51)Int.Cl. H04L 9/08
H04L 12/28

(21)Application number : 2000-317630
(22)Date of filing : 18.10.2000

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : TOKINIWA YASUHISA
ATOZAWA SHINOBU

(54) ENCRYPTION COMMUNICATION SYSTEM AND METHOD FOR DELIVERING ENCODING KEY

(57)Abstract:
PROBLEM TO BE SOLVED: To alleviate a load on a network at delivery responding of an encoding key used for an encryption communication group.
SOLUTION: A group encryption key managing unit 1 generates a group key, and transmits the key to terminal units T2 to T6 belonging to a communication group 13 via a router 5 and a router 8. The terminal units T2 to T6 transmit delivery response data D3 for transmitting reception of the group key to the router 5. The router 5 transmits the data as a simultaneous response data D4 to the unit 1 based on the data D3. The units T5 and T6 transmit the data D3 for transmitting the reception of the key to the router 8. The router 8 transmits the data D3 to the unit 1 as the data D4 based on the data D3.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－124941
(P2002－124941A)
(43)公開日　平成14年４月26日(2002.4.26)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	５Ｊ１０４
12/28		11/00	３１０Ｚ	５Ｋ０３３

審査請求　未請求　請求項の数12　ＯＬ　（全 22 頁）

(21)出願番号　特願2000－317630(P2000－317630)

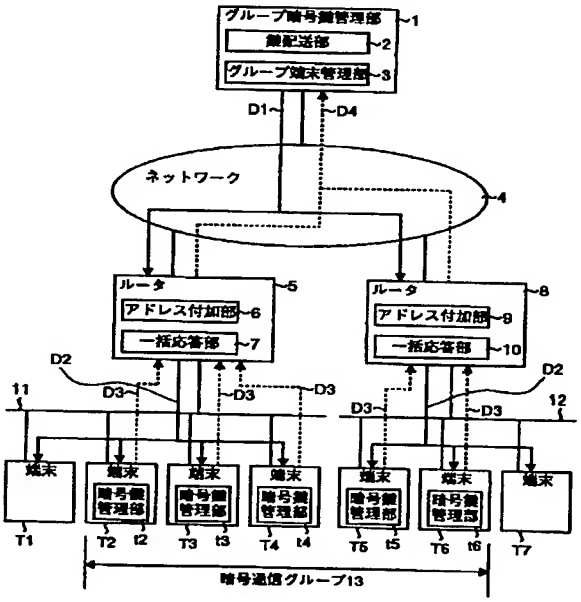
(22)出願日　平成12年10月18日(2000.10.18)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　時庭　康久
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　後沢　忍
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100089118
弁理士　酒井　宏明

Ｆターム(参考)　5J104 AA16 BA02 EA01 EA04 EA18 MA06 NA02 PA07
5K033 AA03 AA08 BA13 CB01 DA03

(54)【発明の名称】　暗号通信システムおよび暗号鍵配送方法

(57)【要約】
【課題】　暗号通信グループが用いる暗号鍵の配送応答時におけるネットワークの負担を軽減すること。
【解決手段】グループ暗号鍵管理部１がグループ暗号鍵を生成し、ルータ５およびルータ８を介して暗号通信グループ１３に属する端末Ｔ２～Ｔ６に送信する。端末Ｔ２～Ｔ４は、グループ暗号鍵を受信したことを伝える配送応答データＤ３をルータ５に送信し、ルータ５は、配送応答データＤ３をもとに、一括応答データＤ４としてグループ暗号鍵管理部１に送信する。端末Ｔ５，Ｔ６は、グループ暗号鍵を受信したことを伝える配送応答データＤ３をルータ８に送信し、ルータ８は、配送応答データＤ３をもとに、一括応答データＤ４としてグループ暗号鍵管理部１に送信する。



【特許請求の範囲】

【請求項１】　グループ暗号鍵を用いた暗号通信が行われる暗号通信グループを形成する複数の端末が中継手段を介してネットワークに接続され、該ネットワークに接続されたグループ暗号鍵管理手段が前記グループ暗号鍵を生成し、前記中継手段を介して各端末に配送する暗号通信システムにおいて、
前記グループ暗号鍵管理手段は、
前記生成したグループ暗号鍵を含む鍵配送データを前記各端末に一斉に送信する鍵配送手段と、
前記中継手段から受信した一括応答データをもとに、前記暗号通信グループを形成する前記各端末が前記グループ暗号鍵を受信したか否かを管理するグループ端末管理手段とを備え、
前記中継手段は、
前記鍵配送データに代理応答アドレスとして自中継手段のアドレスを付加し、鍵配送終端データとして自中継手段が中継する前記端末に送信するアドレス付加手段と、
前記端末から受信した配送応答データをもとに、前記グループ暗号鍵を受信した端末の情報を含む前記一括応答データを前記グループ暗号鍵管理手段に送信する一括応答手段とを備え、
前記端末は、
前記鍵配送終端データを受信して前記グループ暗号鍵を受信し、自端末の情報を含む前記配送応答データを前記中継手段に送信する暗号鍵管理手段を備えることを特徴とする暗号通信システム。

【請求項２】　前記一括応答手段は、前記一括応答データに含まれる端末の情報を暗号化する第１の暗号化手段をさらに備え、
前記グループ端末管理手段は、前記一括応答データに含まれる暗号化された端末の情報を復号する第１の復号手段をさらに備えることを特徴とする請求項１に記載の暗号通信システム。

【請求項３】　前記暗号鍵管理手段は、前記配送応答データに含まれる自端末の情報を暗号化する第２の暗号化手段をさらに備え、
前記一括応答手段は、前記配送応答データに含まれる暗号化された情報を復号する第２の復号手段をさらに備えることを特徴とする請求項１または２に記載の暗号通信システム。

【請求項４】　前記第１の暗号化手段、前記第２の暗号化手段、前記第１の復号手段、および前記第２の復号手段は、秘密鍵暗号方式によってそれぞれ暗号化または復号を行うことを特徴とする請求項２または３に記載の暗号通信システム。

【請求項５】　前記第１の暗号化手段、前記第２の暗号化手段、前記第１の復号手段、および前記第２の復号手段は、公開鍵暗号方式によってそれぞれ暗号化または復号を行うことを特徴とする請求項２または３に記載の暗号通信システム。

【請求項６】　前記第１の暗号化手段、前記第２の暗号化手段、前記第１の復号手段、および前記第２の復号手段は、既に配送されたグループ暗号鍵を少なくとも保持し、この保持されたグループ暗号鍵のうちの所定のグループ暗号鍵を用いて暗号化または復号を行うことを特徴とする請求項２～４のいずれか一つに記載の暗号通信システム。

【請求項７】　グループ暗号鍵を用いた暗号通信が行われる暗号通信グループを形成する複数の端末が中継手段を介してネットワークに接続され、該ネットワークに接続されたグループ暗号鍵管理手段が前記グループ暗号鍵を生成し、前記中継手段を介して各端末に配送する暗号鍵配送方法において、
前記グループ暗号鍵管理手段が、前記グループ暗号鍵を含む鍵配送データを前記端末に一斉に送信する鍵配送データ送信工程と、
前記中継手段が、前記鍵配送データに代理応答アドレスとして自中継手段のアドレスを付加し、該アドレスが付加された鍵配送データを鍵配送終端データとして前記端末に送信する鍵配送終端データ送信工程と、
前記端末が、前記鍵配送終端データを受信して前記グループ暗号鍵を受信し、自端末の情報を含む配送応答データを前記中継手段に送信する配送応答データ送信工程と、
前記中継手段が、前記端末から受信した配送応答データをもとに、前記グループ暗号鍵を受信した端末の情報を含む一括応答データを前記グループ暗号鍵管理手段に送信する一括応答データ送信工程と、
前記グループ暗号鍵管理手段が、前記一括応答データをもとに、前記各端末が前記グループ暗号鍵を受信したか否かを確認する配送結果確認工程と、
を含むことを特徴とする暗号鍵配送方法。

【請求項８】　前記一括応答データ送信工程は、前記一括応答データに含まれる端末の情報を暗号化する第１の暗号化工程をさらに含み、
前記配送結果確認工程は、前記一括応答データに含まれる暗号化された端末の情報を復号する第１の復号工程をさらに含むことを特徴とする請求項７に記載の暗号鍵配送方法。

【請求項９】　前記配送応答データ送信工程は、前記配送応答データに含まれる自端末の情報を暗号化する第２の暗号化工程をさらに含み、
前記一括応答データ送信工程は、前記配送応答データに含まれる暗号化された情報を復号する第２の復号工程をさらに含むことを特徴とする請求項７または８に記載の暗号鍵配送方法。

【請求項１０】　前記第１の暗号化工程、前記第２の暗号化工程、前記第１の復号工程、および前記第２の復号工程は、秘密鍵暗号方式によってそれぞれ暗号化または

復号を行うことを特徴とする請求項８または９に記載の暗号鍵配送方法。

【請求項１１】　前記第１の暗号化工程、前記第２の暗号化工程、前記第１の復号工程、および前記第２の復号工程は、公開鍵暗号方式によってそれぞれ暗号化または復号を行うことを特徴とする請求項８または９に記載の暗号鍵配送方法。

【請求項１２】　前記第１の暗号化工程、前記第２の暗号化工程、前記第１の復号工程、および前記第２の復号工程は、既に配送されたグループ暗号鍵を少なくとも保持し、この保持されたグループ暗号鍵のうちの所定のグループ暗号鍵を用いて暗号化または復号を行うことを特徴とする請求項８または９に記載の暗号鍵配送方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、グループ暗号鍵を用いた暗号通信が行われる暗号通信グループを形成する複数の端末が中継手段を介してネットワークに接続され、該ネットワークに接続されたグループ暗号鍵管理手段が前記グループ暗号鍵を生成し、前記中継手段を介して各端末に配送する暗号通信システムおよび暗号鍵配送方法に関し、特に、ネットワークの負担を軽減することができる暗号通信システムおよび暗号鍵配送方法に関するものである。

【０００２】

【従来の技術】従来から、ネットワークに接続された端末間の通信における安全性を確保するために、端末をグループ分けし、同一のグループ内の通信を共通の暗号鍵を用いて行う暗号通信システムがある。この共通の暗号鍵は、安全性を高めるためにしばしば更新されるが、新しい暗号鍵自体も安全に各端末に配送しなければならない。

【０００３】図８は、従来の暗号通信システムの構成を示す図である。この従来の暗号通信システムは、グループ暗号鍵管理部８０１と複数の端末８１０，８２０，８３０を有し、グループ暗号鍵管理部８０１が各端末８１０，８２０，８３０にグループ暗号鍵８０２を配送する。ここでは、端末８１０，８２０，８３０が、１つの暗号通信グループを形成しているものとする。グループ暗号鍵８０２の配送は、暗号化されて行われる。このため、グループ暗号鍵管理部８０１および各端末８１０，８２０，８３０は、配送用暗号鍵を、たとえば物理的に安全な方法で配布するなど、なんらかの手段で予め秘密に共有していなければならない。暗号通信グループに対してグループ暗号鍵を配送する場合、グループ暗号鍵を配送するグループ暗号鍵管理部８０１と各端末８１０，８２０，８３０とは、配送用暗号鍵を、それぞれ配送用暗号鍵保持部８０５，８１３に保持していなければならない。

【０００４】暗号化部８０３および復号部８１４は、配送用暗号鍵保持部８０５，８１３から入力された配送用暗号鍵を用いてグループ暗号鍵８０２をそれぞれ暗号化し、復号する。暗号方式としては、暗号化と復号とで同じ暗号鍵を用いる秘密鍵暗号方式を採用する。この秘密鍵暗号方式には、たとえば米国の標準暗号方式であるＤＥＳ（Data Encryption Standard）などがあるが、暗号鍵を知らない者が暗号文から平文を推定できない方式であればよい。なお、ＥＮＣ（Ｍ，Ｋ）およびＤＥＣ（Ｍ，Ｋ）は、鍵Ｋを用いて情報Ｍをそれぞれ暗号化し、復号する関数を表す。また、同報送信部８０６は、各端末８１０，８２０，８３０に同報送信する。また、同報受信部８１１は、同報送信部８０６から送られた同報情報を受信する。

【０００５】つぎに、図９に示すフローチャートを用いてグループ暗号鍵配送時のグループ暗号鍵管理部８０１の動作を説明する。ある暗号通信グループにおける暗号通信の開始時に（ステップＳ１０１）、グループ暗号鍵管理部８０１は、まずグループ暗号鍵を生成する（ステップＳ１０２）。つぎに暗号通信グループ内の各端末それぞれについて（ステップＳ１０３）、該端末との配送用暗号鍵を配送用暗号鍵保持部８０５から順次取出し（ステップＳ１０４）、それぞれの配送用暗号鍵を鍵として暗号化部８０３でグループ暗号鍵を順次暗号化して暗号化グループ暗号鍵を計算し（ステップＳ１０５）、それらをグループ暗号鍵リスト８０４にまとめて（ステップＳ１０６）、同報送信部８０６が該リストをマルチキャスト送信する（ステップＳ１０７）。該リストは、全端末に受信される。マルチキャスト送信には、ＩＧＭＰ（Internet Group Management Protocol ）などの標準的な通信規約を用いることができる。

【０００６】つぎに、図１０を用いてグループ暗号鍵配送時の端末の動作を説明する。端末８１０が同報受信部８１１によりグループ暗号鍵リスト８０４を受信した場合（ステップＳ２０１）、グループ暗号鍵リスト８０４に自端末に対応する暗号化グループ暗号鍵があれば（ステップＳ２０２，Ｙｅｓ）、グループ暗号鍵リスト８０４から暗号化グループ暗号鍵を取り出し（ステップＳ２０３）、配送用暗号鍵保持部８１３に保持されたグループ暗号鍵管理部８０１との配送用暗号鍵を取り出し（ステップＳ２０４）、配送用暗号鍵を用いて復号部８１４で暗号化グループ暗号鍵を復号し、グループ暗号鍵８０２を得る（ステップＳ２０５）。一方、受信したグループ暗号鍵リスト８０４の中に自端末に対応する暗号化グループ暗号鍵がない場合には（ステップＳ２０２，Ｎｏ）、グループ暗号鍵リスト８０４を無視する（ステップＳ２０６）。

【０００７】つぎに、図１１を用いてグループ暗号鍵リストについて具体的に説明する。グループ暗号鍵管理部８０１と端末８１０，８２０，８３０とはそれぞれ配送用暗号鍵Ｋ８１０，Ｋ８２０，Ｋ８３０を保持してい

る。グループ暗号鍵管理部８０１はグループ暗号鍵Ｘを生成し、各端末８１０，８２０，８３０との配送用暗号鍵Ｋ８１０、Ｋ８２０、Ｋ８３０をそれぞれ鍵として、グループ暗号鍵Ｘを暗号化し、暗号化されたグループ暗号鍵Ｙ８１０、Ｙ８２０、Ｙ８３０を作成する。

【０００８】すなわちグループ暗号鍵管理部８０１は

Ｙ８１０＝ＥＮＣ（Ｘ，Ｋ８１０）

Ｙ８２０＝ＥＮＣ（Ｘ，Ｋ８２０）

Ｙ８３０＝ＥＮＣ（Ｘ，Ｋ８３０）

を生成する。その後、グループ暗号鍵管理部８０１はグループ暗号鍵Ｙ８１０，Ｙ８２０，Ｙ８３０をグループ暗号鍵リスト９０１（図１１参照）として全端末８１０，８２０，８３０にマルチキャスト送信する。グループ暗号鍵リスト８０４は暗号通信グループに属さない端末や第三者に受信されても、その端末に対応する配送用暗号鍵がないのでグループ暗号鍵Ｘを推察されることはない。

【０００９】一方、グループ暗号鍵管理部８０１からグループ暗号鍵リスト８０４に対応するグループ暗号鍵リスト９０１を受け取った端末８１０は、グループ暗号鍵リスト９０１から自端末に対応する暗号化グループ暗号鍵Ｙ８１０を取り出し、グループ暗号鍵管理部８０１との配送用暗号鍵Ｋ８１０を鍵として用いて復号を行い、グループ暗号鍵Ｘを得る。

【００１０】端末８２０、端末８３０についても同様な復号処理を行い各端末８１０，８２０，８３０では次のよう復号結果を得る。

端末８１０：Ｘ＝ＤＥＣ（Ｙ８１０，Ｋ８１０）

端末８２０：Ｘ＝ＤＥＣ（Ｙ８２０，Ｋ８２０）

端末８３０：Ｘ＝ＤＥＣ（Ｙ８３０，Ｋ８３０）

これによって、端末８１０，８２０，８３０のみがグループ暗号鍵Ｘを受信し、グループ通信用の暗号鍵として保持し、使用する。グループ暗号鍵Ｘの受信後、端末８１０，８２０，８３０は、配送結果を一斉にグループ暗号鍵管理部８０１に応答する。グループ暗号鍵管理部８０１は、暗号通信グループに属する端末８１０，８２０，８３０からの配送応答によって、どの端末が正常にグループ暗号鍵Ｘを受信したかを知る。これによって、暗号通信グループに属するグループ暗号鍵管理部８０１，端末８１０，８２０，８３０は、グループ暗号鍵Ｘを共有することができる。

【００１１】

【発明が解決しようとする課題】しかしながら、上述した暗号通信システムは、グループ暗号鍵を受信した端末が、グループ暗号鍵管理部への配送応答を一斉に行うので、暗号通信グループの規模が大きくなり、端末数が増えると、グループ暗号鍵管理部での負荷が増大し、通信ネットワーク上の通信量が大きくなるという問題点があった。また、グループ暗号鍵の配送応答のセキュリティ強度を高めて暗号通信システムの安全性を高める必要があった。

【００１２】この発明は上記に鑑みてなされたものであって、暗号通信グループがグループ暗号鍵の共有を容易に行い、かつ、ネットワークの負担を軽減し、さらにセキュリティを強化した暗号通信システムおよび暗号鍵配送方法を得ることを目的とする。

【００１３】

【課題を解決するための手段】上記目的を達成するため、この発明にかかる暗号通信システムは、グループ暗号鍵を用いた暗号通信が行われる暗号通信グループを形成する複数の端末が中継手段を介してネットワークに接続され、該ネットワークに接続されたグループ暗号鍵管理手段が前記グループ暗号鍵を生成し、前記中継手段を介して各端末に配送する暗号通信システムにおいて、前記グループ暗号鍵管理手段は、前記生成したグループ暗号鍵を含む鍵配送データを前記各端末に一斉に送信する鍵配送手段と、前記中継手段から受信した一括応答データをもとに、前記暗号通信グループを形成する前記各端末が前記グループ暗号鍵を受信したか否かを管理するグループ端末管理手段とを備え、前記中継手段は、前記鍵配送データに代理応答アドレスとして自中継手段のアドレスを付加し、鍵配送終端データとして自中継手段が中継する前記端末に送信するアドレス付加手段と、前記端末から受信した配送応答データをもとに、前記グループ暗号鍵を受信した端末の情報を含む前記一括応答データを前記グループ暗号鍵管理手段に送信する一括応答手段とを備え、前記端末は、前記鍵配送終端データを受信して前記グループ暗号鍵を受信し、自端末の情報を含む前記配送応答データを前記中継手段に送信する暗号鍵管理手段を備えることを特徴とする。

【００１４】この発明によれば、中継手段は、グループ暗号鍵管理手段が送信した鍵配送データに、自中継手段のアドレスを付加して各端末に配送し、各端末は、受信したデータに付加されたアドレスをもとに、自端末の情報を含む配送応答データを中継手段に送信し、中継手段は、端末から受信した配送応答データをもとに、グループ暗号鍵を受信した端末の情報をまとめ、一括応答データとしてグループ暗号鍵管理手段に送信する。

【００１５】つぎの発明にかかる暗号通信システムは、上記の発明において、前記一括応答手段は、前記一括応答データに含まれる端末の情報を暗号化する第１の暗号化手段をさらに備え、前記グループ端末管理手段は、前記一括応答データに含まれる暗号化された端末の情報を復号する第１の復号手段をさらに備えることを特徴とする。

【００１６】この発明によれば、中継手段はグループ暗号鍵を受信した端末の情報を暗号化してグループ暗号鍵管理手段に送信し、グループ暗号鍵管理手段は、中継手段からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができる。

【００１７】つぎの発明にかかる暗号通信システムは、上記の発明において、前記暗号鍵管理手段は、前記配送応答データに含まれる自端末の情報を暗号化する第２の暗号化手段をさらに備え、前記一括応答手段は、前記配送応答データに含まれる暗号化された情報を復号する第２の復号手段をさらに備えることを特徴とする。

【００１８】この発明によれば、各端末は、グループ暗号鍵を受信した場合に自端末の情報を暗号化して中継手段に送信し、中継手段は、各端末からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができる。

【００１９】つぎの発明にかかる暗号通信システムは、上記の発明において、前記第１の暗号化手段、前記第２の暗号化手段、前記第１の復号手段、および前記第２の復号手段は、秘密鍵暗号方式によってそれぞれ暗号化または復号を行うことを特徴とする。

【００２０】この発明によれば、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、秘密鍵暗号方式で暗号化され、送受信される。

【００２１】つぎの発明にかかる暗号通信システムは、上記の発明において、前記第１の暗号化手段、前記第２の暗号化手段、前記第１の復号手段、および前記第２の復号手段は、公開鍵暗号方式によってそれぞれ暗号化または復号を行うことを特徴とする。

【００２２】この発明によれば、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、公開鍵暗号方式で暗号化され、送受信される。

【００２３】つぎの発明にかかる暗号通信システムは、上記の発明において、前記第１の暗号化手段、前記第２の暗号化手段、前記第１の復号手段、および前記第２の復号手段は、既に配送されたグループ暗号鍵を少なくとも保持し、この保持されたグループ暗号鍵のうちの所定のグループ暗号鍵を用いて暗号化または復号を行うことを特徴とする。

【００２４】この発明によれば、グループ暗号鍵が更新される場合に、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、使用していたグループ暗号鍵で暗号化され、送受信される。

【００２５】つぎの発明にかかる暗号鍵配送方法は、グループ暗号鍵を用いた暗号通信が行われる暗号通信グループを形成する複数の端末が中継手段を介してネットワークに接続され、該ネットワークに接続されたグループ暗号鍵管理手段が前記グループ暗号鍵を生成し、前記中継手段を介して各端末に配送する暗号鍵配送方法において、前記グループ暗号鍵管理手段が、前記グループ暗号鍵を含む鍵配送データを前記端末に一斉に送信する鍵配送データ送信工程と、前記中継手段が、前記鍵配送データに代理応答アドレスとして自中継手段のアドレスを付加し、該アドレスが付加された鍵配送データを鍵配送終端データとして前記端末に送信する鍵配送終端データ送信工程と、前記端末が、前記鍵配送終端データを受信して前記グループ暗号鍵を受信し、自端末の情報を含む配送応答データを前記中継手段に送信する配送応答データ送信工程と、前記中継手段が、前記端末から受信した配送応答データをもとに、前記グループ暗号鍵を受信した端末の情報を含む一括応答データを前記グループ暗号鍵管理手段に送信する一括応答データ送信工程と、前記グループ暗号鍵管理手段が、前記一括応答データをもとに、前記各端末が前記グループ暗号鍵を受信したか否かを確認する配送結果確認工程と、を含むことを特徴とする。

【００２６】この発明によれば、中継手段は、グループ暗号鍵管理手段が送信した鍵配送データに、自中継手段のアドレスを付加して各端末に送信し、各端末は、受信したデータに付加されたアドレスをもとに、自端末の情報を含む配送応答データを中継手段に送信し、中継手段は、端末から受信した配送応答データをもとにグループ暗号鍵を受信した端末の情報をまとめ、一括応答データとしてグループ暗号鍵管理手段に送信する。

【００２７】つぎの発明にかかる暗号鍵配送方法は、前記一括応答データ送信工程は、前記一括応答データに含まれる端末の情報を暗号化する第１の暗号化工程をさらに含み、前記配送結果確認工程は、前記一括応答データに含まれる暗号化された端末の情報を復号する第１の復号工程をさらに含むことを特徴とする。

【００２８】この発明によれば、中継手段はグループ暗号鍵を受信した端末の情報を暗号化してグループ暗号鍵管理手段に送信し、グループ暗号鍵管理手段は、中継手段からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができる。

【００２９】つぎの発明にかかる暗号鍵配送方法は、上記の発明において、前記配送応答データ送信工程は、前記配送応答データに含まれる自端末の情報を暗号化する第２の暗号化工程をさらに含み、前記一括応答データ送信工程は、前記配送応答データに含まれる暗号化された情報を復号する第２の復号工程をさらに含むことを特徴とする。

【００３０】この発明によれば、各端末は、グループ暗号鍵を受信した場合に自端末の情報を暗号化して中継手段に送信し、中継手段は、各端末からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができる。

【００３１】つぎの発明にかかる暗号鍵配送方法は、上記の発明において、前記第１の暗号化工程、前記第２の暗号化工程、前記第１の復号工程、および前記第２の復号工程は、秘密鍵暗号方式によってそれぞれ暗号化または復号を行うことを特徴とする。

【００３２】この発明によれば、一括応答データに含ま

れる端末の情報、および配送応答データに含まれる自端末の情報は、秘密鍵暗号方式で暗号化され、送受信される。

【００３３】つぎの発明にかかる暗号鍵配送方法は、上記の発明において、前記第１の暗号化工程、前記第２の暗号化工程、前記第１の復号工程、および前記第２の復号工程は、公開鍵暗号方式によってそれぞれ暗号化または復号を行うことを特徴とする。

【００３４】この発明によれば、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、公開鍵暗号方式で暗号化され、送受信される。

【００３５】つぎの発明にかかる暗号鍵配送方法は、上記の発明において、前記第１の暗号化工程、前記第２の暗号化工程、前記第１の復号工程、および前記第２の復号工程は、既に配送されたグループ暗号鍵を少なくとも保持し、この保持されたグループ暗号鍵のうちの所定のグループ暗号鍵を用いて暗号化または復号を行うことを特徴とする。

【００３６】この発明によれば、グループ暗号鍵が更新される場合に、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、使用していたグループ暗号鍵で暗号化され、送受信される。

【００３７】

【発明の実施の形態】以下に添付図面を参照して、この発明に係る暗号通信システムおよび暗号鍵配送方法の好適な実施の形態を詳細に説明する。

【００３８】実施の形態１．図１は、この発明の第１の実施の形態である暗号通信システムの構成を示す図である。図１において、暗号通信システムは、グループ暗号鍵管理部１、中継手段としての機能を有するルータ５，８が、ネットワーク４に接続されている。ルータ５はさらにＬＡＮ１１を介して端末Ｔ１～Ｔ４に接続される。また、ルータ８は、ＬＡＮ１２を介して端末Ｔ５～Ｔ７と接続されている。さらに、端末Ｔ２～Ｔ６は、暗号通信グループ１３に含まれている。なお、ネットワーク４は、電話網や、ＩＳＤＮ網などを含んでもよい。

【００３９】グループ暗号鍵管理部１は、暗号通信グループ１３が暗号通信に用いるグループ暗号鍵を生成する。グループ暗号鍵管理部１は、生成したグループ暗号鍵を含む鍵配送データＤ１を暗号通信グループに属する各端末Ｔ２～Ｔ６にマルチキャスト送信する鍵配送部２と、一括応答データＤ４をもとに暗号通信グループに属する各端末Ｔ２～Ｔ６の情報を管理するグループ端末管理部３を有している。

【００４０】ルータ５はグループ暗号鍵管理部１が送信した鍵配送データＤ１に、代理応答アドレスとしてルータ５のＩＰアドレスを付加して鍵配送終端データＤ２を作成するアドレス付加部６を有し、ＬＡＮ１１に接続された端末Ｔ１～Ｔ４に鍵配送終端データＤ２を送信する。また、ルータ５は、暗号通信グループ１３に属する端末Ｔ２～Ｔ４がグループ暗号鍵を受信した場合に送出する配送応答データＤ３をもとに、グループ暗号鍵を受信した端末の情報を暗号化し、グループ暗号鍵管理部１に一括応答データＤ４として送信する一括応答部７を有する。

【００４１】また、ルータ８は、ルータ５と同様に、グループ暗号鍵管理部１が送信した鍵配送データＤ１に、代理応答アドレスとしてルータ８のＩＰアドレスを付加して鍵配送終端データＤ２を作成するアドレス付加部９を有し、ＬＡＮ１２に接続された端末Ｔ５～Ｔ７に鍵配送終端データＤ２を送信する。さらに、ルータ８は、暗号通信グループ１３に属する端末Ｔ５～Ｔ６がグループ暗号鍵を受信した場合に送出する配送応答データＤ３をもとに、グループ暗号鍵を受信した端末の情報を暗号化し、グループ暗号鍵管理部１に一括応答データＤ４として送信する一括応答部１０を有する。

【００４２】端末Ｔ２は、鍵配送終端データＤ２を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データＤ３としてルータ５に送信する暗号鍵管理部ｔ２を有する。端末Ｔ３，Ｔ４は、端末Ｔ２と同様に鍵配送終端データＤ２を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データＤ３としてルータ５に送信する暗号鍵管理部ｔ３，ｔ４を有する。なお、端末Ｔ１は、ＬＡＮ１１に接続されているが、暗号通信グループ１３には属さない。

【００４３】端末Ｔ５，Ｔ６は、鍵配送終端データＤ２を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データＤ３としてルータ８に送信する暗号鍵管理部ｔ５，ｔ６を有する。なお、端末Ｔ７は、ＬＡＮ１１に接続されているが、暗号通信グループ１３には属さない。

【００４４】さらに、グループ暗号鍵管理部１の鍵配送部２とグループ端末管理部３、ルータ５の一括応答部７、ルータ８の一括応答部１０および端末Ｔ２～Ｔ６の暗号鍵管理部ｔ２～ｔ６は、秘密鍵暗号に用いる暗号鍵ＫＣＣを共有している。秘密鍵暗号にはたとえば米国の標準暗号方式ＤＥＳ（Data Encryption Standard）などがあるが、暗号鍵を知らない者が暗号文から平文を推定できないようなものならいかなる方式でもよい。

【００４５】ここで、図２を参照して、鍵配送データＤ１、鍵配送終端データＤ２、配送応答データＤ３、一括応答データＤ４についてさらに詳細に説明する。

【００４６】鍵配送データＤ１は、グループ暗号鍵管理部１の鍵配送部２によって作成される。鍵配送データＤ１は、送信元ＩＰアドレス、宛先ＩＰアドレス、データ種別、グループ識別子、グループ暗号鍵データを有する。鍵配送部２は、鍵配送データＤ１の送信元ＩＰアドレスにグループ暗号鍵管理部１のＩＰアドレスを設定し、宛先ＩＰアドレスには暗号通信グループ１３のマル

チキャストアドレスを設定し、データ種別には鍵配送を設定し、グループ識別子には暗号通信グループ１３を識別するＩＤ１３を設定し、グループ暗号鍵データにグループ暗号鍵管理部１が作成したグループ暗号鍵ＫＳＥを設定する。さらに、グループ識別子およびグループ暗号鍵を、暗号鍵ＫＣＣで暗号化している。

【００４７】鍵配送終端データＤ２は、鍵配送データＤ１をもとに、ルータのアドレス付加部によって作成される。鍵配送終端データＤ２は、送信元ＩＰアドレス、宛先ＩＰアドレス、データ種別、グループ識別子、グループ暗号鍵データ、代理応答アドレス、を有する。鍵配送終端データＤ２には、ルータのアドレス付加部が鍵配送データＤ１に代理応答アドレスとして自己のＩＰアドレスを付加している。すなわち、ルータ５のアドレス付加部６は、代理応答アドレスとしてルータ５のＩＰアドレスを付加し、ルータ８のアドレス付加部９は、代理応答アドレスとしてルータ８のＩＰアドレスを付加する。また、鍵配送終端データＤ２の、送信元ＩＰアドレス、宛先ＩＰアドレス、暗号化されたグループ識別子およびグループ暗号鍵データは、鍵配送データＤ１から変更されず、データ種別は、鍵配送から鍵配送終端に書き替えられる。

【００４８】配送応答データＤ３は、鍵配送終端データＤ２をもとに、端末の暗号鍵管理部によって作成される。配送応答データＤ３は、送信元ＩＰアドレス、宛先ＩＰアドレス、データ種別、グループ識別子、配送済み端末ＩＰアドレス、を有する。端末の暗号鍵管理部は、鍵配送終端データＤ２を受信し、暗号化されたグループ識別子およびグループ暗号鍵データを暗号鍵ＫＣＣで復号し、グループ暗号鍵ＫＳＥを取り出し、グループ暗号鍵を正常に受信したことを示す配送応答データＤ３を作成する。具体的には、送信元ＩＰアドレスに自端末のＩＰアドレスを設定し、宛先アドレスに鍵配送終端データＤ２の代理応答アドレスに設定されたルータのＩＰアドレスを設定し、データ種別に配送応答を設定し、グループ識別子に暗号通信グループ１３を識別するＩＤ１３を設定し、配送済み端末ＩＰアドレスに自端末のＩＰアドレスを設定する。さらに、グループ識別子および配送済み端末ＩＰアドレスは暗号鍵ＫＣＣで暗号化される。

【００４９】すなわち、端末Ｔ２の暗号鍵管理部ｔ２は、送信元ＩＰアドレスおよび配送済み端末ＩＰアドレスに端末Ｔ２のＩＰアドレスを設定し、宛先ＩＰアドレスにはルータ５のＩＰアドレスを設定する。また、端末Ｔ３およびＴ４の暗号鍵管理部ｔ３およびｔ４も同様に送信元ＩＰアドレスおよび配送済み端末ＩＰアドレスに自端末のＩＰアドレスを設定し、宛先ＩＰアドレスにルータ５のＩＰアドレスを設定する。さらに、端末Ｔ５およびＴ６においても同様である。端末Ｔ５およびＴ６では、鍵配送終端データＤ２はルータ８から受信しており、代理応答アドレスはルータ８のＩＰアドレスであるため、宛先ＩＰアドレスはルータ８のＩＰアドレスとなる。また、端末Ｔ１および端末Ｔ７は、暗号通信グループ１３に属さず、受信した鍵配送終端データＤ２を破棄する。

【００５０】一括応答データＤ４は、各端末から受信した配送応答データＤ３をもとに、ルータの一括応答部によって作成される。一括応答データＤ４は、送信元ＩＰアドレス、宛先ＩＰアドレス、データ種別、グループ識別子、配送済み有効数、配送済み端末複数ＩＰアドレスを有する。ルータの一括応答部は、ルータが鍵配送終端データＤ２を送信してから一定時間内に受信した配送応答データＤ３のグループ識別子および配送済み端末ＩＰアドレスを暗号鍵ＫＣＣで復号し、グループ暗号鍵を正常に受信した端末の数と、各端末のＩＰアドレスとを得る。さらに一括応答部は、送信元ＩＰアドレスに自ルータのＩＰアドレスを設定し、宛先ＩＰアドレスにグループ鍵管理部１のＩＰアドレスを設定し、データ種別に一括応答を設定し、グループ識別子に暗号通信グループ１３を識別するＩＤ１３を設定し、配送済み有効数にグループ暗号鍵を正常に受信した端末の数を設定し、配送済み端末複数ＩＰアドレスにグループ暗号鍵を正常に受信した各端末のＩＰアドレスを設定する。さらに、グループ識別子、配送済み有効数、配送済み端末複数ＩＰアドレスを暗号鍵ＫＣＣで暗号化する。

【００５１】具体的には、ルータ５の一括応答部７は、端末Ｔ２、端末Ｔ３、端末Ｔ４からそれぞれ配送応答データＤ３を受信し、各配送応答データＤ３の暗号化されたグループ識別子および配送済み端末ＩＰアドレスを暗号鍵ＫＣＣで復号し、端末Ｔ２、端末Ｔ３、端末Ｔ４のＩＰアドレスを得る。さらに一括応答部７は、送信元ＩＰアドレスにルータ５のＩＰアドレスを設定し、宛先ＩＰアドレスにグループ暗号鍵管理部１のＩＰアドレスを設定し、データ種別に一括応答を設定し、グループ識別子に暗号通信グループ１３を識別するＩＤ１３を設定し、配送済み有効数に３を設定し、配送済み端末複数ＩＰアドレスに端末Ｔ２、Ｔ３、Ｔ４のＩＰアドレスをそれぞれ設定し、グループ識別子、配送済み有効数、配送済み端末複数ＩＰアドレスを暗号鍵ＫＣＣで暗号化する。

【００５２】また、ルータ８の一括応答部１０は、端末Ｔ５およびＴ６からそれぞれ配送応答データＤ３を受信し、各配送応答データＤ３の暗号化されたグループ識別子および配送済み端末ＩＰアドレスを暗号鍵ＫＣＣで復号し、端末Ｔ５および端末Ｔ６のＩＰアドレスを得る。さらに一括応答部１０は、送信元ＩＰアドレスにルータ８のＩＰアドレスを設定し、宛先ＩＰアドレスにグループ暗号鍵管理部１のＩＰアドレスを設定し、データ種別に一括応答を設定し、グループ識別子に暗号通信グループ１３を識別するＩＤ１３を設定し、配送済み有効数に２を設定し、配送済み端末複数ＩＰアドレスに端末Ｔ５

およびＴ６のＩＰアドレスを設定し、グループ識別子、配送済み有効数、配送済み端末複数ＩＰアドレスを暗号鍵ＫＣＣで暗号化する。

【００５３】つぎに、図３に示すタイミングシーケンスを参照して、グループ暗号鍵の配送についてさらに説明する。

【００５４】まず、グループ暗号鍵管理部１は、グループ暗号鍵ＫＳＥを生成する。鍵配送部２は、暗号鍵ＫＣＣでグループ暗号鍵ＫＳＥを暗号化してＫＣＣ（ＫＳＥ）を作成し、

グループ暗号鍵管理部１：ＫＣＣ（ＫＳＥ）＝ＥＮＣ（ＫＳＥ，ＫＣＣ）

鍵配送データＤ１として各端末にマルチキャスト送信する。

【００５５】ルータ５は、鍵配送データＤ１を受信し、代理応答アドレスとしてルータ５のＩＰアドレスを付加し、鍵配送終端データＤ２としてＬＡＮ１１に接続された端末Ｔ１～Ｔ４に配送する。データＤ２には、暗号鍵ＫＣＣで暗号化されたグループ鍵暗号、KCC（ＫＳＥ）が含まれる。

【００５６】ルータ８は、鍵配送データＤ１を受信し，代理応答アドレスとしてルータ８のＩＰアドレスを付加し、鍵配送終端データＤ２としてＬＡＮ１２に接続された端末Ｔ５～Ｔ７に配送する。鍵配送終端データＤ２には、暗号鍵ＫＣＣで暗号化されたグループ鍵暗号、ＫＣＣ（ＫＳＥ）が含まれる。

【００５７】端末Ｔ１は、鍵配送終端データＤ２を受信するが、暗号通信グループ１３に属さず、暗号鍵ＫＣＣを有さないので、鍵配送終端データＤ２に含まれるＫＣＣ（ＫＳＥ）を復号することはできない。

【００５８】端末Ｔ２は、鍵配送終端データＤ２を受信し、暗号鍵ＫＣＣを用いてＫＣＣ（ＫＳＥ）を復号し、グループ暗号鍵ＫＳＥを得る。

端末Ｔ２：ＫＳＥ＝ＤＥＣ（ＫＣＣ（ＫＳＥ），ＫＣＣ）

さらに、端末Ｔ２は、端末Ｔ２のＩＰアドレスであるＩＰ（Ｔ２）を暗号鍵ＫＣＣで暗号化してＫＣＣ（ＩＰ（Ｔ２））を作成し、

端末Ｔ２：ＫＣＣ（ＩＰ（Ｔ２））＝ＥＮＣ（ＩＰ（Ｔ２），ＫＣＣ）

グループ暗号鍵ＫＳＥを受信したことを伝える配送応答データＤ３を作成し、ルータ５に送信する。

【００５９】端末Ｔ３およびＴ４は、端末Ｔ２と同様に、鍵配送終端データＤ２を受信し、暗号鍵ＫＣＣを用いてＫＣＣ（ＫＳＥ）を復号してグループ暗号鍵ＫＳＥを得る。

端末Ｔ３：ＫＳＥ＝ＤＥＣ（ＫＣＣ（ＫＳＥ），ＫＣＣ）

端末Ｔ４：ＫＳＥ＝ＤＥＣ（ＫＣＣ（ＫＳＥ），ＫＣＣ）

また、端末Ｔ３およびＴ４は、各端末のＩＰアドレスを暗号鍵ＫＣＣで暗号化する。

端末Ｔ３：ＫＣＣ（ＩＰ（Ｔ３））＝ＥＮＣ（ＩＰ（Ｔ３），ＫＣＣ）

端末Ｔ４：ＫＣＣ（ＩＰ（Ｔ４））＝ＥＮＣ（ＩＰ（Ｔ４），ＫＣＣ）

グループ暗号鍵ＫＳＥを受信したことを伝える配送応答データＤ３を作成し、ルータ５に送信する。

【００６０】端末Ｔ５およびＴ６は、端末Ｔ２～Ｔ４と同様に、鍵配送終端データＤ２を受信し、暗号鍵ＫＣＣを用いてＫＣＣ（ＫＳＥ）を復号してグループ暗号鍵ＫＳＥを得る。

端末Ｔ５：ＫＳＥ＝ＤＥＣ（ＫＣＣ（ＫＳＥ），ＫＣＣ）

端末Ｔ６：ＫＳＥ＝ＤＥＣ（ＫＣＣ（ＫＳＥ），ＫＣＣ）

また、端末Ｔ５およびＴ６は、各端末のＩＰアドレスを暗号鍵ＫＣＣで暗号化し、

端末Ｔ５：ＫＣＣ（ＩＰ（Ｔ５））＝ＥＮＣ（ＩＰ（Ｔ５），ＫＣＣ）

端末Ｔ６：ＫＣＣ（ＩＰ（Ｔ６））＝ＥＮＣ（ＩＰ（Ｔ６），ＫＣＣ）

グループ暗号鍵ＫＳＥを受信したことを伝える配送応答データＤ３を作成し、ルータ８に送信する。

【００６１】端末Ｔ７は、鍵配送終端データＤ２を受信するが、暗号通信グループ１３に属さず、暗号鍵ＫＣＣを有さないので、鍵配送終端データＤ２に含まれるＫＣＣ（ＫＳＥ）を復号することはできない。

【００６２】ルータ５は、端末Ｔ２～Ｔ４から配送応答データＤ３を受け取り、暗号鍵ＫＣＣで復号し、各端末のＩＰアドレス、ＩＰ（Ｔ２）、ＩＰ（Ｔ３）、ＩＰ（Ｔ４）を得る。

ルータ５：ＩＰ（Ｔ２）＝ＤＥＣ（ＫＣＣ（ＩＰ（Ｔ２）），ＫＣＣ）

ＩＰ（Ｔ３）＝ＤＥＣ（ＫＣＣ（ＩＰ（Ｔ３）），ＫＣＣ）

ＩＰ（Ｔ４）＝ＤＥＣ（ＫＣＣ（ＩＰ（Ｔ４）），ＫＣＣ）

さらにルータ５は、受信したＩＰアドレスの数３と、各端末のＩＰアドレス、ＩＰ（Ｔ２）、ＩＰ（Ｔ３）、ＩＰ（Ｔ４）を、暗号鍵ＫＣＣで暗号化し、一括応答データＤ４としてグループ暗号鍵管理部１に送信する。

【００６３】ルータ８は、端末Ｔ５およびＴ６から配送応答データＤ３を受け取り、暗号鍵ＫＣＣで復号し、各端末のＩＰアドレス、ＩＰ（Ｔ５）、ＩＰ（Ｔ６）を得る。

ルータ８：ＩＰ（Ｔ５）＝ＤＥＣ（ＫＣＣ（ＩＰ（Ｔ５）），ＫＣＣ）

ＩＰ（Ｔ６）＝ＤＥＣ（ＫＣＣ（ＩＰ（Ｔ６）），ＫＣＣ）

さらにルータ８は、受信したＩＰアドレスの数２と、各端末のＩＰアドレス、ＩＰ（Ｔ５）、ＩＰ（Ｔ６）を暗号鍵ＫＣＣで暗号化し、一括応答データＤ４としてグループ暗号鍵管理部１に送信する。

【００６４】グループ暗号鍵管理部１はルータ５およびルータ８から受信した一括応答データＤ４を暗号鍵ＫＣＣで復号し、グループ暗号鍵ＫＳＥを受信した端末Ｔ２～Ｔ６のＩＰアドレスを得ることができる。

【００６５】このようにして、グループ暗号鍵ＫＳＥは、暗号通信グループ１３に属する各端末に共有される。したがって、暗号通信グループ１３に属する端末、たとえば端末Ｔ６が、グループ暗号鍵ＫＳＥを用いて秘密鍵暗号方式で通信データを暗号化し、暗号通信グループ１３に属する端末にマルチキャスト送信した場合には、端末Ｔ２～Ｔ５は、グループ暗号鍵ＫＳＥで受信したデータを復号することができる。

【００６６】この実施の形態１では、グループ暗号鍵ＫＳＥが配送された場合に、暗号通信グループ１３に属する端末Ｔ２～Ｔ６は、グループ暗号鍵管理部１に直接配送応答をするのではなく、各端末からルータに配送応答をし、ルータが端末の配送応答データをまとめ、一括してグループ暗号鍵管理部１に配送応答をする。したがって、直接各端末からグループ暗号鍵管理部に配送応答をする場合に比べてネットワーク４に送信される通信量は減少し、ネットワークの負荷を少なくすることができる。

【００６７】また、この実施の形態１では、グループ暗号鍵管理部１と、ルータ５および８と、端末Ｔ２～Ｔ６と、で暗号鍵ＫＣＣを共有し、グループ暗号鍵ＫＳＥの配送応答および一括応答を秘密鍵暗号方式で暗号化している。したがって、グループ暗号鍵の配送応答のセキュリティを高めることができる。

【００６８】なお、この実施の形態１では、配送応答データＤ３および一括応答データＤ４に配送済み端末ＩＰアドレスを有していたが、必ずしもＩＰアドレスである必要はなく、グループ暗号鍵管理部で端末を識別する固有の番号でもよい。たとえば、ＩＰアドレスのかわりに、ＭＡＣアドレスや、端末の製造番号を用いても同様の効果を奏することができる。

【００６９】また、この実施の形態１では、グループ暗号鍵ＫＳＥの配送、配送応答、一括応答のすべてに同一の暗号鍵ＫＣＣを用いて暗号化を行っているが、それぞれ異なる暗号鍵を用いて暗号化するようにしてもよいし、ネットワークやＬＡＮのセキュリティの状況によっては、とくに暗号化を行わなくてもよい。

【００７０】実施の形態２．つぎに、この発明の実施の形態２について説明する。この実施の形態２では、グループ暗号鍵を受信した端末は、自端末の情報を公開鍵暗号方式で暗号化してルータに送信し、ルータは端末から受信した情報を復号し、一括してグループ暗号鍵管理部に送信している。

【００７１】図４は、この発明の実施の形態２である暗号通信システムの構成を示す図である。図４において暗号通信システムは、実施の形態１に示した暗号通信システムと同様に、グループ暗号鍵管理部４０、中継手段としての機能を有するルータ４２およびルータ４４が、ネットワーク４に接続されている。ルータ４２はさらにＬＡＮ１１を介して端末Ｔ１～Ｔ４と接続されている。また、ルータ４４は、ＬＡＮ１２を介して端末Ｔ５～Ｔ７と接続されている。さらに、端末Ｔ２～Ｔ６は、暗号通信グループ１３に含まれている。

【００７２】グループ暗号鍵管理部４０は、暗号通信グループ１３が暗号通信に用いるグループ暗号鍵を生成する。グループ暗号鍵管理部４０は、生成したグループ暗号鍵を含む鍵配送データＤ１を暗号通信グループに属する各端末にマルチキャスト送信する鍵配送部２と、一括応答データＤ６をもとに暗号通信グループに属する各端末の情報を管理するグループ端末管理部４１を有している。

【００７３】ルータ４２は、グループ暗号鍵管理部４０が送信した鍵配送データＤ１に、代理応答アドレスとしてルータ４２のＩＰアドレスを付加して鍵配送終端データＤ２を作成するアドレス付加部６を有し、ＬＡＮ１１に接続された端末Ｔ１～Ｔ４に鍵配送終端データＤ２を送信する。また、ルータ４２は、暗号通信グループ１３に属する端末Ｔ２～Ｔ４がグループ暗号鍵を受信した場合に送出する配送応答データＤ５をもとに、グループ暗号鍵を受信した端末の情報を暗号化し、グループ暗号鍵管理部１に一括応答データＤ６として送信する一括応答部４３を有する。

【００７４】また、ルータ４４もルータ４２と同様に、グループ暗号鍵管理部４０が送信した鍵配送データＤ１に、代理応答アドレスとしてルータ４４のＩＰアドレスを付加して鍵配送終端データＤ２を作成するアドレス付加部９を有し、ＬＡＮ１２に接続された端末Ｔ５～Ｔ７に鍵配送終端データＤ２を送信する。さらに、ルータ４４は、暗号通信グループ１３に属する端末Ｔ５およびＴ６がグループ暗号鍵を受信した場合に送出する配送応答データＤ５をもとに、グループ暗号鍵を受信した端末の情報を暗号化し、グループ暗号鍵管理部４０に一括応答データＤ６として送信する一括応答部４５を有する。

【００７５】端末Ｔ２は、鍵配送終端データＤ２を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データＤ５としてルータ４２に送信する暗号鍵管理部ｔ４２を有する。端末Ｔ３，Ｔ４は、同様に鍵配送終端データＤ２を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データＤ５としてルータ４２に送信する暗号鍵管理部ｔ４３，ｔ４４を有する。

【００７６】端末Ｔ５、Ｔ６は、鍵配送終端データＤ２

を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データＤ５としてルータ４４に送信する暗号鍵管理部ｔ４５、ｔ４６を有する。

【００７７】さらに、グループ暗号鍵管理部４０の鍵配送部２、および端末Ｔ２～Ｔ６の暗号鍵管理部ｔ４２～ｔ４６は、秘密鍵暗号に用いる暗号鍵ＫＣＣを共有している。秘密鍵暗号にはたとえば米国の標準暗号方式ＤＥＳ（Data Encryption Standard）などがあるが、暗号鍵を知らない者が暗号文から平文を推定できないようなものならいかなる方式でもよい。

【００７８】また、ルータ４２の一括応答部４３は、公開鍵暗号に用いる秘密鍵ＫＳ４２を保持しており、端末Ｔ２～Ｔ４の暗号鍵管理部ｔ４２～ｔ４４は、秘密鍵ＫＳ４２に対応する公開鍵ＫＰ４２を保持している。同様に、ルータ４４の一括応答部４５は、公開鍵暗号に用いる秘密鍵ＫＳ４４を保持しており、端末Ｔ５～Ｔ６の暗号鍵管理部ｔ４５～ｔ４６は、秘密鍵ＫＳ４４に対応する公開鍵ＫＰ４４を保持している。

【００７９】さらに、グループ暗号鍵管理部４０のグループ端末管理部４１は、公開鍵暗号に用いる秘密鍵ＫＳ４０を保持しており、ルータ４２の一括応答部４３およびルータ４４の一括応答部４５は、秘密鍵ＫＳ４０に対応する公開鍵ＫＰ４０を保持している。公開鍵暗号としては、ＲＳＡ(Rivest Shamir Adleman)暗号や、楕円Elgamal暗号などを用いることができる。

【００８０】つぎに、鍵配送データＤ１、鍵配送終端データＤ２、配送応答データＤ５、一括応答データＤ６について説明する。鍵配送データＤ１および鍵配送終端データＤ２については、実施の形態１に示した鍵配送データおよび鍵配送終端データと同様である。

【００８１】配送応答データＤ５は、実施の形態１に示した配送応答データＤ３に対応し、公開鍵暗号方式でグループ識別子および配送済み端末ＩＰアドレスを暗号化する。すなわち、端末Ｔ２～Ｔ４の暗号鍵管理部ｔ４２～ｔ４４は、ルータ４２に対応し、公開鍵ＫＰ４２を用いて暗号化を行う。また、端末Ｔ５およびＴ６の暗号鍵管理部ｔ４５およびｔ４６は、ルータ４４に対応し、公開鍵ＫＰ４４を用いて暗号化を行う。

【００８２】一括応答データＤ６は、実施の形態１に示した一括応答データＤ４に対応し、公開鍵暗号方式でグループ識別子、配送済み有効数、配送済み端末複数ＩＰアドレスを暗号化する。すなわち、ルータ４２およびルータ４４は、公開鍵ＫＰ４０を用いて暗号化を行う。

【００８３】つぎに、図５に示すタイミングシーケンスを参照して、グループ暗号鍵の配送についてさらに説明する。

【００８４】まず、グループ暗号鍵管理部４０は、グループ暗号鍵ＫＳＥを生成する。鍵配送部２は、暗号鍵ＫＣＣでグループ暗号鍵ＫＳＥを暗号化してＫＣＣ（ＫＳＥ）を作成し、グループ暗号鍵管理部４０：ＫＣＣ（ＫＳＥ）＝ＥＮＣ（ＫＳＥ，ＫＣＣ）鍵配送データＤ１として各端末にマルチキャスト送信する。

【００８５】ルータ４２は、鍵配送データＤ１を受信し、代理応答アドレスとしてルータ４２のＩＰアドレスを付加し、鍵配送終端データＤ２としてＬＡＮ１１に接続された端末Ｔ１～Ｔ４に配送する。データＤ２には、暗号鍵ＫＣＣで暗号化されたグループ鍵暗号、ＫＣＣ（ＫＳＥ）が含まれる。

【００８６】ルータ４４は、鍵配送データＤ１を受信し、代理応答アドレスとしてルータ４４のＩＰアドレスを付加し、鍵配送終端データＤ２としてＬＡＮ１２に接続された端末Ｔ５～Ｔ７に配送する。鍵配送終端データＤ２には、暗号鍵ＫＣＣで暗号化されたグループ鍵暗号、ＫＣＣ（ＫＳＥ）が含まれる。

【００８７】端末Ｔ１は、鍵配送終端データＤ２を受信するが、暗号通信グループ１３に属さず、暗号鍵ＫＣＣを有さないので、鍵配送終端データＤ２に含まれるＫＣＣ（ＫＳＥ）を復号することはできない。

【００８８】端末Ｔ２は、鍵配送終端データＤ２を受信し、暗号鍵ＫＣＣを用いてＫＣＣ（ＫＳＥ）を復号し、グループ暗号鍵ＫＳＥを得る。

端末Ｔ２：ＫＳＥ＝ＤＥＣ（ＫＣＣ（ＫＳＥ），ＫＣＣ）

さらに、端末Ｔ２は、端末Ｔ２のＩＰアドレスであるＩＰ（Ｔ２）を公開鍵ＫＰ４２で暗号化してＫＰ４２（ＩＰ（Ｔ２））を作成し、

端末Ｔ２：ＫＰ４２（ＩＰ（Ｔ２））＝ＥＮＣ（ＩＰ（Ｔ２），ＫＰ４２）

グループ暗号鍵ＫＳＥを受信したことを伝える配送応答データＤ５を作成し、ルータ４２に送信する。

【００８９】端末Ｔ３およびＴ４も、端末Ｔ２と同様に、鍵配送終端データＤ２を受信し、暗号鍵ＫＣＣを用いてＫＣＣ（ＫＳＥ）を復号してグループ暗号鍵ＫＳＥを得る。

端末Ｔ３：ＫＳＥ＝ＤＥＣ（ＫＣＣ（ＫＳＥ），ＫＣＣ）

端末Ｔ４：ＫＳＥ＝ＤＥＣ（ＫＣＣ（ＫＳＥ），ＫＣＣ）

また、端末Ｔ３およびＴ４は、各端末のＩＰアドレスを公開鍵ＫＰ４２で暗号化し、

端末Ｔ３：ＫＰ４２（ＩＰ（Ｔ３））＝ＥＮＣ（ＩＰ（Ｔ３），ＫＰ４２）

端末Ｔ４：ＫＰ４２（ＩＰ（Ｔ４））＝ＥＮＣ（ＩＰ（Ｔ４），ＫＰ４２）

グループ暗号鍵ＫＳＥを受信したことを伝える配送応答データＤ５を作成し、ルータ４２に送信する。

【００９０】端末Ｔ５およびＴ６も、端末Ｔ２～Ｔ４と同様に、鍵配送終端データＤ２を受信し、暗号鍵ＫＣＣを用いてＫＣＣ（ＫＳＥ）を復号してグループ暗号鍵ＫＳＥを得る。

端末Ｔ５：ＫＳＥ＝ＤＥＣ（ＫＣＣ（ＫＳＥ），ＫＣＣ）
端末Ｔ６：ＫＳＥ＝ＤＥＣ（ＫＣＣ（ＫＳＥ），ＫＣＣ）
また、端末Ｔ５およびＴ６は、各端末のＩＰアドレスを公開鍵ＫＰ４４で暗号化し、
端末Ｔ５：ＫＰ４４（ＩＰ（Ｔ５））＝ＥＮＣ（ＩＰ（Ｔ５），ＫＰ４４）
端末Ｔ６：ＫＰ４４（ＩＰ（Ｔ６））＝ＥＮＣ（ＩＰ（Ｔ６），ＫＰ４４）
グループ暗号鍵ＫＳＥを受信したことを伝える配送応答データＤ５を作成し、ルータ４４に送信する。

【００９１】端末Ｔ７は、鍵配送終端データＤ２を受信するが、暗号通信グループ１３に属さず、暗号鍵ＫＣＣを有さないので、鍵配送終端データＤ２に含まれるＫＣＣ（ＫＳＥ）を復号することはできない。

【００９２】ルータ４２は、端末Ｔ２～Ｔ４から配送応答データＤ５を受け取り、秘密鍵ＫＳ４２で復号し、各端末のＩＰアドレス、ＩＰ（Ｔ２）、ＩＰ（Ｔ３）、ＩＰ（Ｔ４）を得る。
ルータ４２：ＩＰ（Ｔ２）＝ＤＥＣ（ＫＰ４２（ＩＰ（Ｔ２）），ＫＳ４２）
ＩＰ（Ｔ３）＝ＤＥＣ（ＫＰ４２（ＩＰ（Ｔ３）），ＫＳ４２）
ＩＰ（Ｔ４）＝ＤＥＣ（ＫＰ４２（ＩＰ（Ｔ４）），ＫＳ４２）
さらにルータ４２は、受信したＩＰアドレスの数３と、各端末のＩＰアドレス、ＩＰ（Ｔ２）、ＩＰ（Ｔ３）、ＩＰ（Ｔ４）を、公開鍵ＫＰ４０で暗号化し、一括応答データＤ６としてグループ暗号鍵管理部４０に送信する。

【００９３】ルータ４４は、端末Ｔ５～Ｔ６から配送応答データＤ５を受け取り、秘密鍵ＫＳ４４で復号し、各端末のＩＰアドレス、ＩＰ（Ｔ５）、ＩＰ（Ｔ６）を得る。
ルータ４４：ＩＰ（Ｔ５）＝ＤＥＣ（ＫＰ４４（ＩＰ（Ｔ５）），ＫＳ４４）
ＩＰ（Ｔ６）＝ＤＥＣ（ＫＰ４４（ＩＰ（Ｔ６）），ＫＳ４４）
さらにルータ４４は、受信したＩＰアドレスの数２と、各端末のＩＰアドレス、ＩＰ（Ｔ５）、ＩＰ（Ｔ６）を公開鍵ＫＰ４０で暗号化し、一括応答データＤ６としてグループ暗号鍵管理部４０に送信する。

【００９４】グループ暗号鍵管理部４０はルータ４２およびルータ４４から受信した一括応答データＤ６を秘密鍵ＫＳ４０で復号し、グループ暗号鍵ＫＳＥを受信した端末Ｔ２～Ｔ６のＩＰアドレスを得ることができる。

【００９５】このようにして、グループ暗号鍵ＫＳＥは、暗号通信グループ１３に属する各端末に共有される。したがって、暗号通信グループ１３に属する端末、たとえば端末Ｔ６が、グループ暗号鍵ＫＳＥを用いて秘密鍵暗号方式で通信データを暗号化し、暗号通信グループ１３に属する端末にマルチキャスト送信した場合には、端末Ｔ２～Ｔ５は、グループ暗号鍵ＫＳＥで受信したデータを復号することができる。

【００９６】この実施の形態２では、グループ暗号鍵ＫＳＥが配送された場合に、暗号通信グループ１３に属する端末Ｔ２～Ｔ６は、グループ暗号鍵管理部４０に直接配送応答をするのではなく、各端末からルータに配送応答をし、ルータが端末の配送応答データをまとめ、一括してグループ暗号鍵管理部４０に配送応答をする。したがって、直接各端末からグループ暗号鍵管理部に配送応答をする場合に比べてネットワーク４に送信される通信量は減少し、ネットワークの負荷を少なくすることができる。

【００９７】また、この実施の形態２では、グループ暗号鍵ＫＳＥの配送応答および一括応答を公開鍵暗号方式で暗号化している。したがって、グループ暗号鍵の配送応答のセキュリティをより高めることができる。

【００９８】なお、この実施の形態２では、配送応答データＤ５および一括応答データＤ６に配送済み端末ＩＰアドレスを有していたが、必ずしもＩＰアドレスである必要はなく、グループ暗号鍵管理部で端末を識別する固有の番号でもよい。たとえば、ＩＰアドレスのかわりに、ＭＡＣアドレスや、端末の製造番号を用いても同様の効果を奏することができる。

【００９９】実施の形態３．つぎに、この発明の実施の形態３について説明する。この実施の形態３では、暗号通信グループに属する各端末は、すでにグループ暗号鍵ＫＳＥＮ０を共有している。暗号鍵管理部６０は、新規のグループ暗号鍵ＫＳＥＮ１を生成し、暗号通信グループに属する各端末に配送し、グループ暗号鍵を更新する。また、新規のグループ暗号鍵の配送、配送応答、一括応答は、既に共有されているグループ暗号鍵ＫＳＥＮ０で暗号化される。

【０１００】図６は、この発明の実施の形態３である暗号通信システムの構成を示す図である。図６において暗号通信システムは、実施の形態１に示した暗号通信システムと同様に、グループ暗号鍵管理部６０、中継手段としての機能を有するルータ６３およびルータ６６が、ネットワーク４に接続されている。ルータ６３はさらにＬＡＮ１１を介して端末Ｔ１、端末Ｔ２、端末Ｔ３および端末Ｔ４と接続されている。また、ルータ６６は、ＬＡＮ１２を介して端末Ｔ５、端末Ｔ６および端末Ｔ７と接続されている。さらに、端末Ｔ２～Ｔ６は、暗号通信グループ１３に含まれている。

【０１０１】グループ暗号鍵管理部６０は、暗号通信グループ１３が暗号通信に用いるグループ暗号鍵を生成する。グループ暗号鍵管理部６０は、生成したグループ暗号鍵を含む鍵配送データＤ６１を暗号通信グループに属

する各端末にマルチキャスト送信する鍵配送部６１と、一括応答データＤ６４をもとに暗号通信グループに属する各端末の情報を管理するグループ端末管理部６２を有している。

【０１０２】ルータ６３は、グループ暗号鍵管理部６０が送信した鍵配送データＤ６１に、代理応答アドレスとしてルータ６３のＩＰアドレスを付加して鍵配送終端データＤ６２を作成するアドレス付加部６４を有し、ＬＡＮ１１に接続された端末Ｔ１～Ｔ４に鍵配送終端データＤ６２を送信する。また、ルータ６３は、暗号通信グループ１３に属する端末Ｔ２～Ｔ４がグループ暗号鍵を受信した場合に送出する配送応答データＤ６３をもとに、グループ暗号鍵を受信した端末の情報を暗号化し、グループ暗号鍵管理部６０に一括応答データＤ６４として送信する一括応答部６５を有する。

【０１０３】また、ルータ６６は、ルータ６３と同様に、グループ暗号鍵管理部６０が送信した鍵配送データＤ６１に、代理応答アドレスとしてルータ６６のＩＰアドレスを付加して鍵配送終端データＤ６２を作成するアドレス付加部６７を有し、ＬＡＮ１２に接続された端末Ｔ５～Ｔ７に鍵配送終端データＤ６２を送信する。さらに、ルータ６６は、暗号通信グループ１３に属する端末Ｔ５～Ｔ６がグループ暗号鍵を受信した場合に送出する配送応答データＤ６３をもとに、グループ暗号鍵を受信した端末の情報を暗号化し、グループ暗号鍵管理部６０に一括応答データＤ６４として送信する一括応答部６８を有する。

【０１０４】端末Ｔ２は、鍵配送終端データＤ６２を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データＤ６３としてルータ６３に送信する暗号鍵管理部ｔ６２を有する。端末Ｔ３，Ｔ４は、同様に鍵配送終端データＤ６２を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データＤ６３としてルータ６３に送信する暗号鍵管理部ｔ６３，ｔ６４を有する。

【０１０５】端末Ｔ５，Ｔ６は、鍵配送終端データＤ６２を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データＤ６３としてルータ６６に送信する暗号鍵管理部ｔ６５，ｔ６６を有する。

【０１０６】さらに、グループ暗号鍵管理部６０の鍵配送部６１、ルータ６３，６６、および端末Ｔ２～Ｔ６の暗号鍵管理部ｔ６２～ｔ６６は、グループ暗号鍵ＫＳＥＮ０を共有している。

【０１０７】つぎに、鍵配送データＤ６１、鍵配送終端データＤ６２、配送応答データＤ６３、一括応答データＤ６４について説明する。

【０１０８】鍵配送データＤ６１は、実施の形態１に示した鍵配送データＤ１に対応し、既に共有されているグループ暗号鍵ＫＳＥＮ０でグループ識別子および配送済み端末のＩＰアドレスを暗号化される。

【０１０９】鍵配送終端データＤ６２は、実施の形態１に示した鍵配送終端データＤ２に対応している。

【０１１０】配送応答データＤ６３は、実施の形態１に示した配送応答データＤ３に対応し、既に共有されているグループ暗号鍵ＫＳＥＮ０でグループ識別子および配送済み端末ＩＰアドレスを暗号化される。

【０１１１】一括応答データＤ６４は、実施の形態１に示した一括応答データＤ４に対応し、既に共有されているグループ暗号鍵ＫＳＥＮ０でグループ識別子、配送済み有効数、配送済み端末複数ＩＰアドレスを暗号化される。

【０１１２】つぎに、図７に示すタイミングシーケンスを参照して、グループ暗号鍵の配送についてさらに説明する。

【０１１３】まず、グループ暗号鍵管理部６０、ルータ６３，６６、端末Ｔ２～Ｔ６は、なんらかの手段でグループ暗号鍵ＫＳＥＮ０をすでに共有している。グループ暗号鍵管理部６０は、新規のグループ暗号鍵ＫＳＥＮ１を生成する。鍵配送部６１は、グループ暗号鍵ＫＳＥＮ０で新規のグループ暗号鍵ＫＳＥＮ１を暗号化してＫＳＥＮ０（ＫＳＥＮ１）を作成し、グループ暗号鍵管理部６０：ＫＳＥＮ０（ＫＳＥＮ１）＝ＥＮＣ（ＫＳＥＮ１，ＫＳＥＮ０）鍵配送データＤ６１として各端末にマルチキャスト送信する。

【０１１４】ルータ６３は、鍵配送データＤ６１を受信し、代理応答アドレスとしてルータ６３のＩＰアドレスを付加し、鍵配送終端データＤ６２としてＬＡＮ１１に接続された端末Ｔ１～Ｔ４に配送する。鍵配送終端データＤ６２には、グループ暗号鍵ＫＳＥＮ０で暗号化された新規のグループ暗号鍵、ＫＳＥＮ０（ＫＳＥＮ１）が含まれる。

【０１１５】ルータ６６は、鍵配送データＤ６１を受信し，代理応答アドレスとしてルータ６６のＩＰアドレスを付加し、鍵配送終端データＤ６２としてＬＡＮ１２に接続された端末Ｔ５～Ｔ７に配送する。鍵配送終端データＤ６２には、グループ暗号鍵ＫＳＥＮ０で暗号化された新規のグループ暗号鍵、ＫＳＥＮ０（ＫＳＥＮ１）が含まれる。

【０１１６】端末Ｔ２は、鍵配送終端データＤ６２を受信し、グループ暗号鍵ＫＳＥＮ０を用いてＫＳＥＮ０（ＫＳＥＮ１）を復号し、新規のグループ暗号鍵ＫＳＥＮ１を得る。

端末Ｔ２：ＫＳＥＮ１＝ＤＥＣ（ＫＳＥＮ０（ＫＳＥＮ１），ＫＳＥＮ０）

さらに、端末Ｔ２は、端末Ｔ２のＩＰアドレスであるＩＰ（Ｔ２）をグループ暗号鍵ＫＳＥＮ０で暗号化してＫＳＥＮ０（ＩＰ（Ｔ２））を作成し、

端末Ｔ２：ＫＳＥＮ０（ＩＰ（Ｔ２））＝ＥＮＣ（ＩＰ（Ｔ２），ＫＳＥＮ０）

新規のグループ暗号鍵ＫＳＥＮ１を受信したことを伝え

る配送応答データＤ６３を作成し、ルータ６３に送信する。

【０１１７】端末Ｔ３およびＴ４は、端末Ｔ２と同様に、鍵配送終端データＤ６２を受信し、グループ暗号鍵ＫＳＥＮ０を用いてＫＳＥＮ０（ＫＳＥＮ１）を復号し、新規のグループ暗号鍵ＫＳＥＮ１を得る。

端末Ｔ３：ＫＳＥＮ１＝ＤＥＣ（ＫＳＥＮ０（ＫＳＥＮ１），ＫＳＥＮ０）

端末Ｔ４：ＫＳＥＮ１＝ＤＥＣ（ＫＳＥＮ０（ＫＳＥＮ１），ＫＳＥＮ０）

また、端末Ｔ３およびＴ４は、各端末のＩＰアドレスをグループ暗号鍵ＫＳＥＮ０で暗号化し、

端末Ｔ３：ＫＳＥＮ０（ＩＰ（Ｔ３））＝ＥＮＣ（ＩＰ（Ｔ３），ＫＳＥＮ０）

端末Ｔ４：ＫＳＥＮ０（ＩＰ（Ｔ４））＝ＥＮＣ（ＩＰ（Ｔ４），ＫＳＥＮ０）

新規のグループ暗号鍵ＫＳＥＮ１を受信したことを伝える配送応答データＤ６３を作成し、ルータ６３に送信する。

【０１１８】端末Ｔ５およびＴ６は、端末Ｔ２～Ｔ４と同様に、鍵配送終端データＤ６２を受信し、グループ暗号鍵ＫＳＥＮ０を用いてＫＳＥＮ０（ＫＳＥＮ１）を復号して新規のグループ暗号鍵ＫＳＥＮ１を得る。

端末Ｔ５：ＫＳＥＮ１＝ＤＥＣ（ＫＳＥＮ０（ＫＳＥＮ１），ＫＳＥＮ０）

端末Ｔ６：ＫＳＥＮ１＝ＤＥＣ（ＫＳＥＮ０（ＫＳＥＮ１），ＫＳＥＮ０）

また、端末Ｔ５およびＴ６は、各端末のＩＰアドレスをグループ暗号鍵ＫＳＥＮ０で暗号化し、

端末Ｔ５：ＫＳＥＮ０（ＩＰ（Ｔ５））＝ＥＮＣ（ＩＰ（Ｔ５），ＫＳＥＮ０）

端末Ｔ６：ＫＳＥＮ０（ＩＰ（Ｔ６））＝ＥＮＣ（ＩＰ（Ｔ６），ＫＳＥＮ０）

新規のグループ暗号鍵ＫＳＥＮ１を受信したことを伝える配送応答データＤ６３を作成し、ルータ６６に送信する。

【０１１９】端末Ｔ７は、鍵配送終端データＤ６２を受信するが、暗号通信グループ１３に属さず、グループ暗号鍵ＫＳＥＮ０を有さないので、鍵配送終端データＤ６２に含まれるＫＳＥＮ０（ＫＳＥＮ１）を復号することはできない。

【０１２０】ルータ６３は、端末Ｔ２～Ｔ４から配送応答データＤ６３を受け取り、グループ暗号鍵ＫＳＥＮ０で復号し、各端末のＩＰアドレス、ＩＰ（Ｔ２）、ＩＰ（Ｔ３）、ＩＰ（Ｔ４）を得る。

ルータ６３：ＩＰ（Ｔ２）＝ＤＥＣ（ＫＳＥＮ０（ＩＰ（Ｔ２）），ＫＳＥＮ０）

ＩＰ（Ｔ３）＝ＤＥＣ（ＫＳＥＮ０（ＩＰ（Ｔ３）），ＫＳＥＮ０）

ＩＰ（Ｔ４）＝ＤＥＣ（ＫＳＥＮ０（ＩＰ（Ｔ４）），ＫＳＥＮ０）

さらにルータ６３は、受信したＩＰアドレスの数３と、各端末のＩＰアドレス、ＩＰ（Ｔ２）、ＩＰ（Ｔ３）、ＩＰ（Ｔ４）を、グループ暗号鍵ＫＳＥＮ０で暗号化し、一括応答データＤ６４としてグループ暗号鍵管理部６０に送信する。

【０１２１】ルータ６６は、端末Ｔ５～Ｔ６から配送応答データＤ６３を受け取り、グループ暗号鍵ＫＳＥＮ０で復号し、各端末のＩＰアドレス、ＩＰ（Ｔ５）、ＩＰ（Ｔ６）を得る。

ルータ６６：ＩＰ（Ｔ５）＝ＤＥＣ（ＫＳＥＮ０（ＩＰ（Ｔ５）），ＫＳＥＮ０）

ＩＰ（Ｔ６）＝ＤＥＣ（ＫＳＥＮ０（ＩＰ（Ｔ６）），ＫＳＥＮ０）

さらにルータ６６は、受信したＩＰアドレスの数２と、各端末のＩＰアドレス、ＩＰ（Ｔ５）、ＩＰ（Ｔ６）をグループ暗号鍵ＫＳＥＮ０で暗号化し、一括応答データＤ６４としてグループ暗号鍵管理部６０に送信する。

【０１２２】グループ暗号鍵管理部６０はルータ６３およびルータ６６から受信した一括応答データＤ６４をグループ暗号鍵ＫＳＥＮ０で復号し、新規のグループ暗号鍵ＫＳＥＮ１を受信した端末Ｔ２～Ｔ６のＩＰアドレスを得ることができる。

【０１２３】このようにして、グループ暗号鍵ＫＳＥＮ１は、暗号通信グループ１３に属する各端末に共有される。したがって、暗号通信グループ１３に属する端末、たとえば端末Ｔ６が、新規のグループ暗号鍵ＫＳＥＮ１を用いて秘密鍵暗号方式で通信データを暗号化し、暗号通信グループ１３に属する端末にマルチキャスト送信した場合には、端末Ｔ２～Ｔ５は、グループ暗号鍵ＫＳＥＮ１で受信したデータを復号することができる。

【０１２４】また、グループ暗号鍵管理部６０が、新たなグループ暗号鍵ＫＳＥＮ２を生成したときには、グループ暗号鍵ＫＳＥＮ１で新たなグループ暗号鍵ＫＳＥＮ２を暗号化して配送することができ、配送応答、一括応答もグループ暗号鍵ＫＳＥＮ１で暗号化することができる。

【０１２５】この実施の形態３では、グループ暗号鍵ＫＳＥＮ１が配送された場合に、暗号通信グループ１３に属する端末Ｔ２～Ｔ６は、グループ暗号鍵管理部６０に直接配送応答をするのではなく、各端末からルータに配送応答をし、ルータが端末の配送応答データをまとめ、一括してグループ暗号鍵管理部６０に配送応答をする。したがって、直接各端末からグループ暗号鍵管理部に配送応答をする場合に比べてネットワーク４に送信される通信量は減少し、ネットワークの負荷を少なくすることができる。

【０１２６】また、この実施の形態３では、新規のグループ暗号鍵ＫＳＥＮ１の配送応答および一括応答を既存のグループ暗号鍵ＫＳＥＮ０で暗号化している。したが

って、グループ暗号鍵の配送応答のセキュリティを高めることができ、また、グループ暗号鍵の更新を容易に行うことができる。

【０１２７】なお、この実施の形態３では、配送応答データＤ６３および一括応答データＤ６４に配送済み端末ＩＰアドレスを有していたが、必ずしもＩＰアドレスである必要はなく、グループ暗号鍵管理部で端末を識別する固有の番号でもよい。たとえば、ＩＰアドレスのかわりに、ＭＡＣアドレスや、端末の製造番号を用いても同様の効果を奏することができる。

【０１２８】

【発明の効果】以上説明したように、この発明によれば、中継手段は、グループ暗号鍵管理手段が送信した鍵配送データに、自中継手段のアドレスを付加して各端末に配送し、各端末は、受信したデータに付加されたアドレスをもとに、自端末の情報を含む配送応答データを中継手段に送信し、中継手段は、端末から受信した配送応答データをもとに、グループ暗号鍵を受信した端末の情報をまとめ、一括応答データとしてグループ暗号鍵管理手段に送信するので、ネットワークへの負担を軽減することができるという効果を奏する。

【０１２９】つぎの発明によれば、中継手段はグループ暗号鍵を受信した端末の情報を暗号化してグループ暗号鍵管理手段に送信し、グループ暗号鍵管理手段は、中継手段からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができるので、グループ暗号鍵を受信した端末の情報を外部に知られることなく、安全にグループ暗号鍵管理手段に送ることができるという効果を奏する。

【０１３０】つぎの発明によれば、各端末は、グループ暗号鍵を受信した場合に自端末の情報を暗号化して中継手段に送信し、中継手段は、各端末からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができるので、端末の情報を外部に知られることなく、安全に中継手段に送ることができるという効果を奏する。

【０１３１】つぎの発明によれば、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、秘密鍵暗号方式で暗号化され、送受信されるので、グループ暗号鍵を受信した端末の情報を安全かつ簡易に送信することができるという効果を奏する。

【０１３２】つぎの発明によれば、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、公開鍵暗号方式で暗号化され、送受信されるので、グループ暗号鍵を受信した端末の情報をより安全に送信することができるという効果を奏する。

【０１３３】つぎの発明によれば、グループ鍵暗号が更新される場合に、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、使用していたグループ暗号鍵で暗号化され、送受信されるので、新規のグループ暗号鍵の配送と、新規のグループ暗号鍵を受信した端末の情報の送信を安全に行うことができ、グループ暗号鍵の更新を安全かつ容易に行うことができるという効果を奏する。

【０１３４】つぎの発明によれば、中継手段は、グループ暗号鍵管理手段が送信した鍵配送データに、自中継手段のアドレスを付加して各端末に送信し、各端末は、受信したデータに付加されたアドレスをもとに、自端末の情報を含む配送応答データを中継手段に送信し、中継手段は、端末から受信した配送応答データをもとにグループ暗号鍵を受信した端末の情報をまとめ、一括応答データとしてグループ暗号鍵管理手段に送信するので、ネットワークへの負担を軽減することができるという効果を奏する。

【０１３５】つぎの発明によれば、中継手段はグループ暗号鍵を受信した端末の情報を暗号化してグループ暗号鍵管理手段に送信し、グループ暗号鍵管理手段は、中継手段からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができるので、グループ暗号鍵を受信した端末の情報を外部に知られることなく、安全にグループ暗号鍵管理手段に送ることができるという効果を奏する。

【０１３６】つぎの発明によれば、各端末は、グループ暗号鍵を受信した場合に自端末の情報を暗号化して中継手段に送信し、中継手段は、各端末からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができるので、端末の情報を外部に知られることなく、安全に中継手段に送ることができるという効果を奏する。

【０１３７】つぎの発明によれば、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、秘密鍵暗号方式で暗号化され、送受信されるので、グループ暗号鍵を受信した端末の情報を安全かつ簡易に送信することができるという効果を奏する。

【０１３８】つぎの発明によれば、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、公開鍵暗号方式で暗号化され、送受信されるので、グループ暗号鍵を受信した端末の情報をより安全に送信することができるという効果を奏する。

【０１３９】この発明によれば、グループ暗号鍵が更新される場合に、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、使用していたグループ暗号鍵で暗号化され、送受信されるので、新規のグループ暗号鍵の配送と、新規のグループ暗号鍵を受信した端末の情報の送信を安全に行うことができ、グループ暗号鍵の更新を安全かつ容易に行うことができるという効果を奏する。

【図面の簡単な説明】

【図１】　この発明の実施の形態１である暗号通信システムの構成を示す図である。

【図２】　図１に示した鍵配送データＤ１、鍵配送終端データＤ２、配送応答データＤ３、一括応答データＤ４

を説明する図である。

【図３】　図１に示した暗号通信システムのタイミングシーケンスを説明する図である。

【図４】　この発明の実施の形態２である暗号通信システムの構成を示す図である。

【図５】　図４に示した暗号通信システムのタイミングシーケンスを説明する図である。

【図６】　この発明の実施の形態３である暗号通信システムの構成を示す図である。

【図７】　図６に示した暗号通信システムのタイミングシーケンスを説明する図である。

【図８】　従来の暗号通信システムの構成を示す図である。

【図９】　図８に示したグループ暗号鍵管理部８０１の動作を説明するフローチャートである。

【図１０】　図８に示した端末の動作を説明するフローチャートである。

【図１１】　グループ暗号鍵リストを説明する図である。

【符号の説明】

１，４０，６０　グループ暗号鍵管理部、２，６１　鍵配送部、３，４１，６２　グループ端末管理部、４　ネットワーク、５，８，４２，４４，６３，６６ルータ、６，９，６４，６７　アドレス付加部、７，１０，４３，４５，６５，６８　一括応答部、１１，１２　ＬＡＮ、１３　暗号通信グループ、Ｄ１，Ｄ６１　鍵配送データ、Ｄ２，Ｄ６２　鍵配送終端データ、Ｄ３，Ｄ５，Ｄ６３配送応答データ、Ｄ４，Ｄ６，Ｄ６４　一括応答データ、Ｔ１～Ｔ７　端末、ｔ２～ｔ６，ｔ４２～ｔ４６，ｔ６２～ｔ６６　暗号鍵管理部、ＫＳＥ，ＫＳＥＮ０，ＫＳＥＮ１，ＫＳＥＮ２　グループ暗号鍵、ＫＣＣ　暗号鍵、ＫＳ４０，ＫＳ４２，ＫＳ４４　秘密鍵、ＫＰ４０，ＫＰ４２，ＫＰ４４　公開鍵。

【図２】

D1　鍵配送データ

送信元 IPアドレス	宛先 IPアドレス		データ種別	グループ識別子	グループ暗号鍵データ
グループ暗号鍵管理部1のIPアドレス	暗号通信グループ13のIPマルチキャストアドレス		鍵配送	ID13	KSE

D2　鍵配送終端データ

送信元 IPアドレス	宛先 IPアドレス		データ種別	グループ識別子	グループ暗号鍵データ	代理応答アドレス
グループ暗号鍵管理部1のIPアドレス	暗号通信グループ13のIPマルチキャストアドレス		鍵配送終端	ID13	KSE	ルータのIPアドレス

D3　配送応答データ

送信元 IPアドレス	宛先 IPアドレス		データ種別	グループ識別子	配送済み端末IPアドレス
端末のIPアドレス	ルータのIPアドレス		配送応答	ID13	端末のIPアドレス

D4　一括応答データ

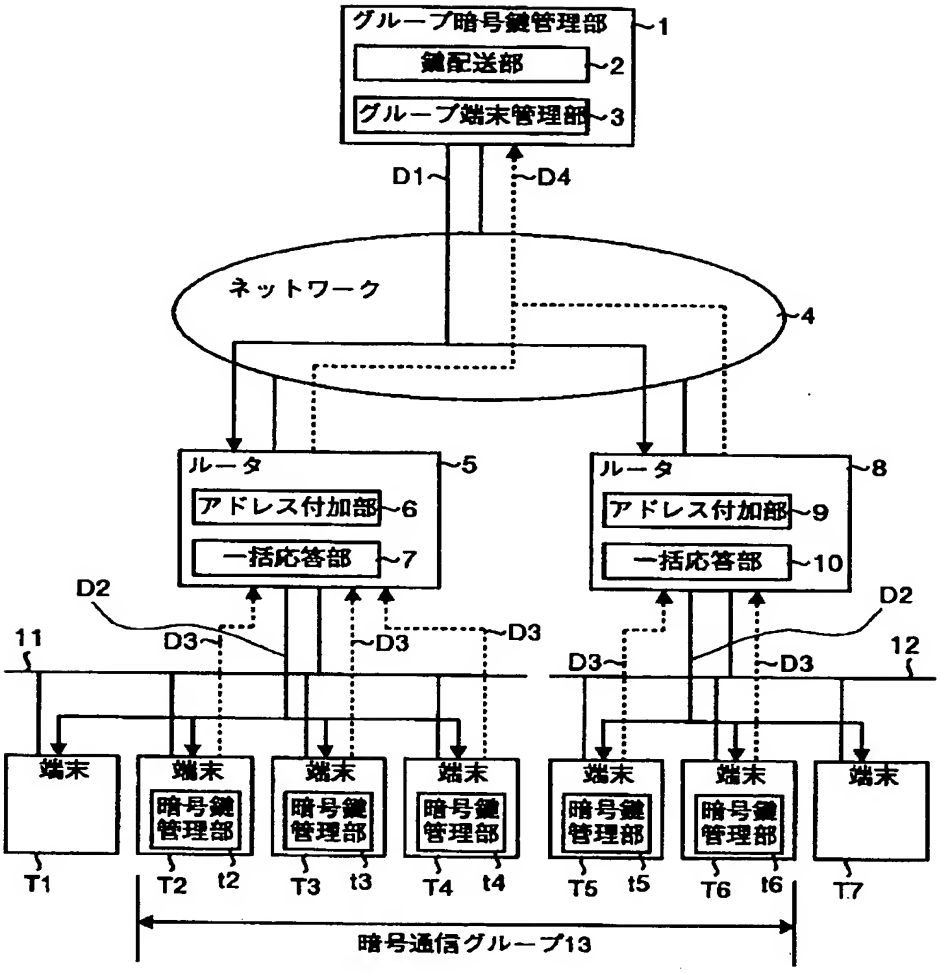
送信元 IPアドレス	宛先 IPアドレス		データ種別	グループ識別子	配送済み有効数	配送済み端末複数IPアドレス		
ルータ5のIPアドレス	グループ暗号鍵管理部1のIPアドレス		一括応答	ID13	3	端末T2のIPアドレス	端末T3のIPアドレス	端末T4のIPアドレス

【図１１】

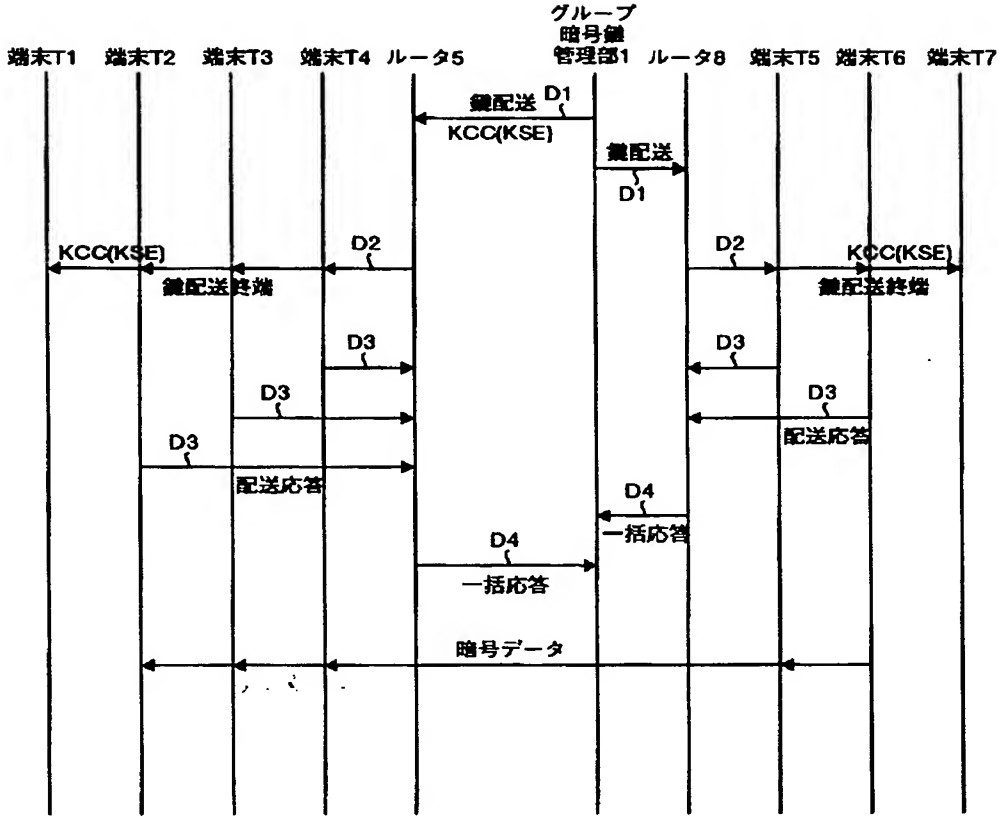
端末12	Y12
端末13	Y13
端末14	Y14
端末21	Y21
端末22	Y22

901

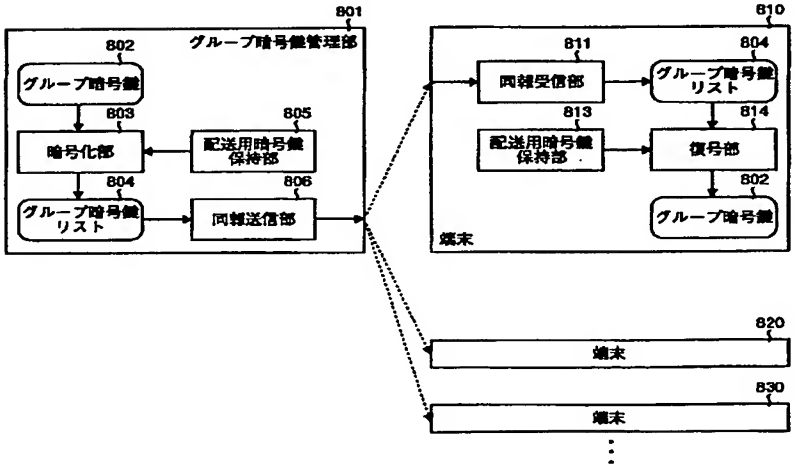
【図１】


グループ暗号鍵管理部
1
鍵配送部
2
グループ端末管理部
3
D1
D4
ネットワーク
4
ルータ
5
アドレス付加部
6
一括応答部
7
ルータ
8
アドレス付加部
9
一括応答部
10
D2
D3
D3
D3
D2
D3
D3
11
12
端末
暗号鍵管理部
T1
T2
t2
T3
t3
T4
t4
T5
t5
T6
t6
T7
暗号通信グループ13

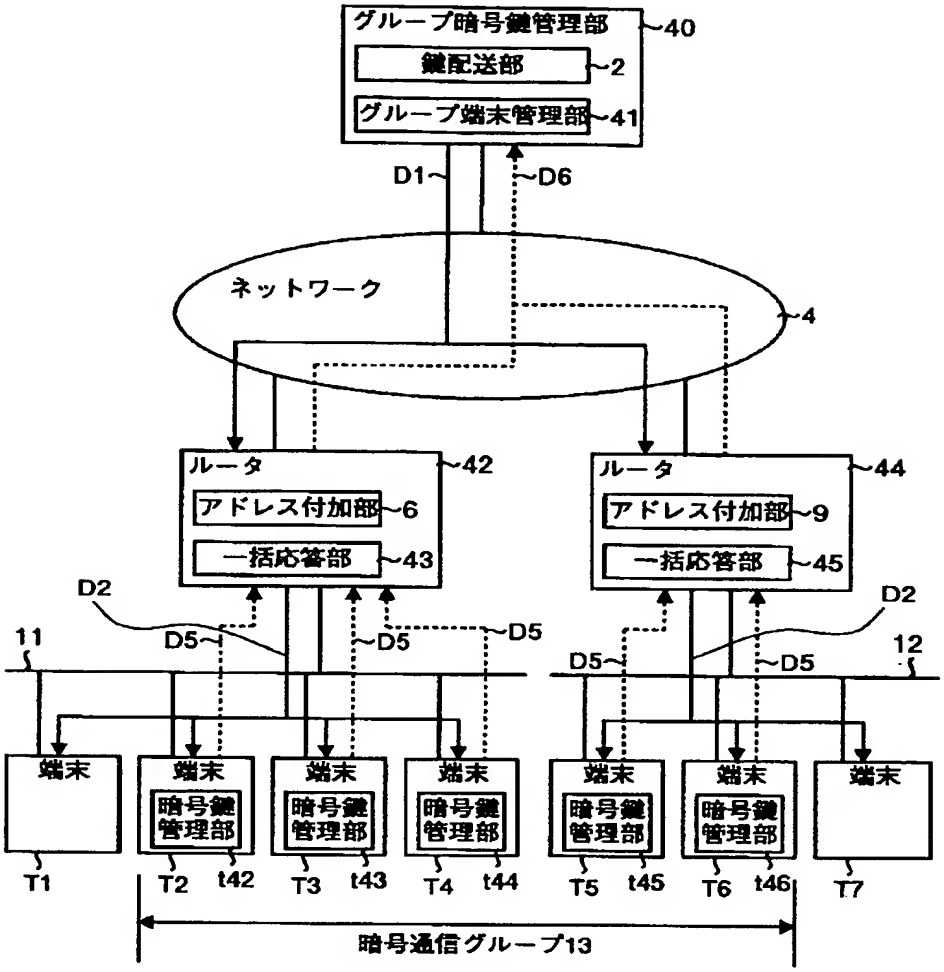
【図３】


グループ
暗号鍵
管理部1
端末T1
端末T2
端末T3
端末T4
ルータ5
ルータ8
端末T5
端末T6
端末T7
鍵配送 D1
KCC(KSE)
鍵配送
D1
KCC(KSE)
鍵配送終端
D2
D2
KCC(KSE)
鍵配送終端
D3
D3
D3
D3
D3
配送応答
D3
配送応答
D4
一括応答
D4
一括応答
暗号データ

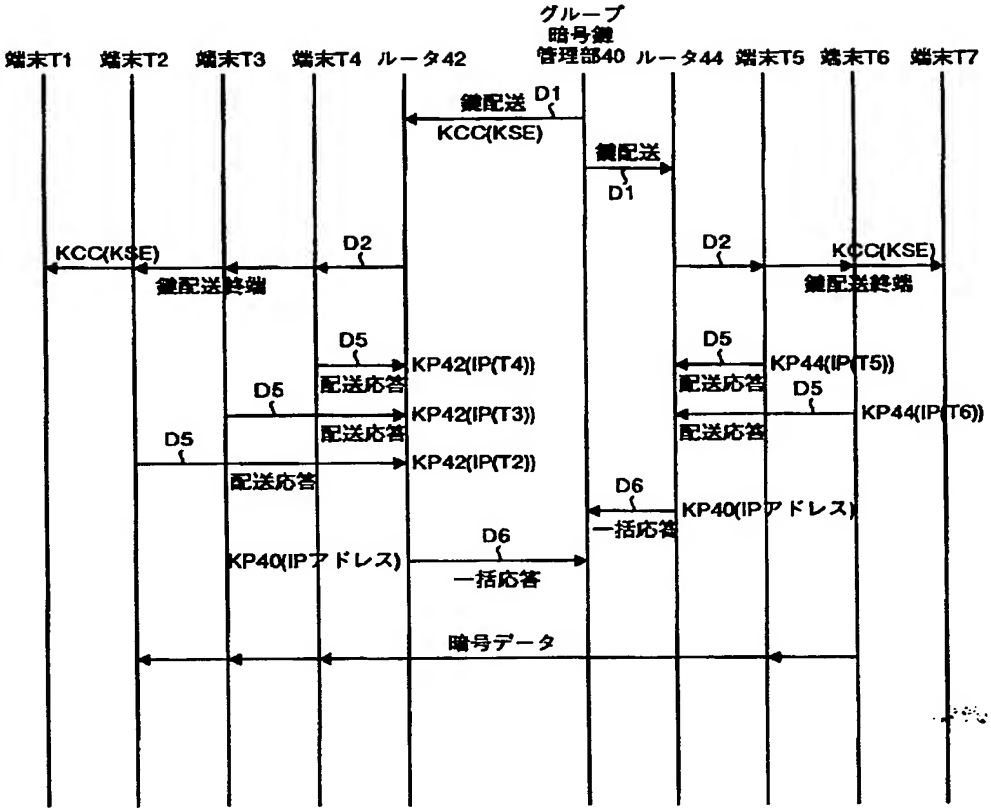
【図８】


801
グループ暗号鍵管理部
802
グループ暗号鍵
803
暗号化部
805
配送用暗号鍵
保持部
804
グループ暗号鍵
リスト
806
同報送信部
810
811
同報受信部
804
グループ暗号鍵
リスト
813
配送用暗号鍵
保持部
814
復号部
802
グループ暗号鍵
端末
820
端末
830
端末

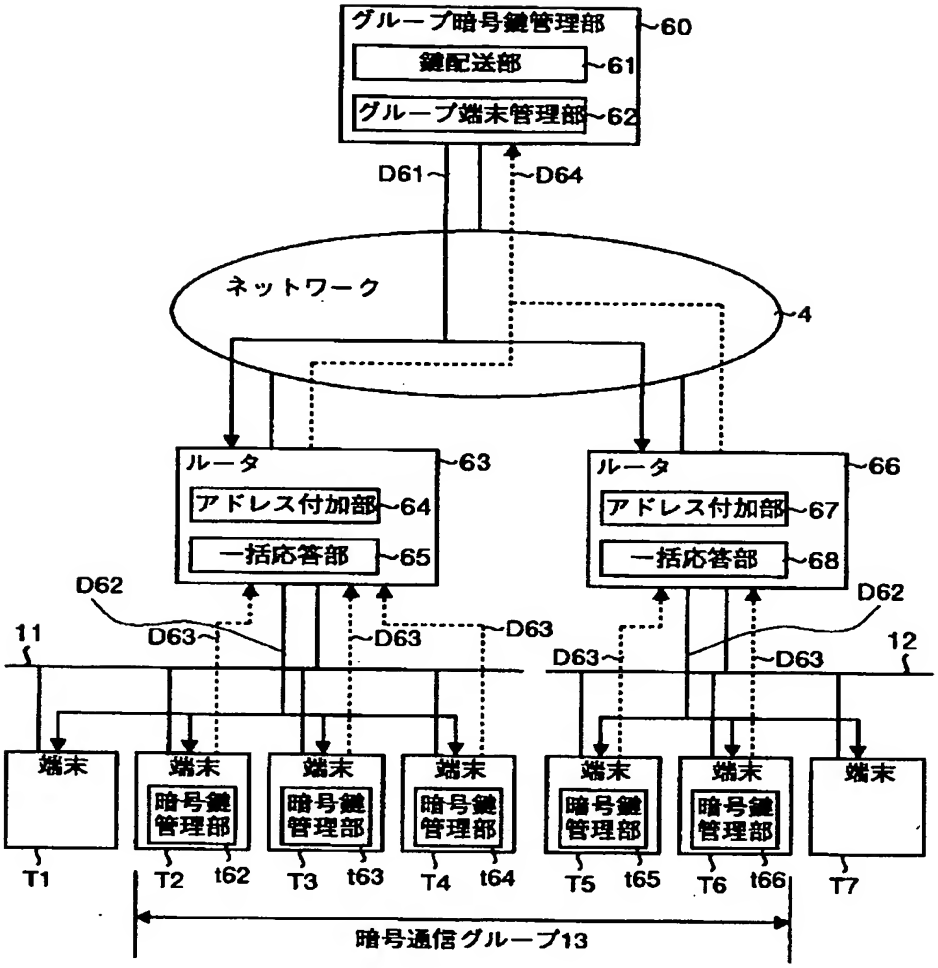
【図４】


グループ暗号鍵管理部
40
鍵配送部
2
グループ端末管理部
41
D1
D6
ネットワーク
4
ルータ
42
アドレス付加部
6
一括応答部
43
ルータ
44
アドレス付加部
9
一括応答部
45
D2
D5
D5
D5
D2
D5
D5
11
12
端末
暗号鍵管理部
T1
T2
t42
T3
t43
T4
t44
T5
t45
T6
t46
T7
暗号通信グループ13

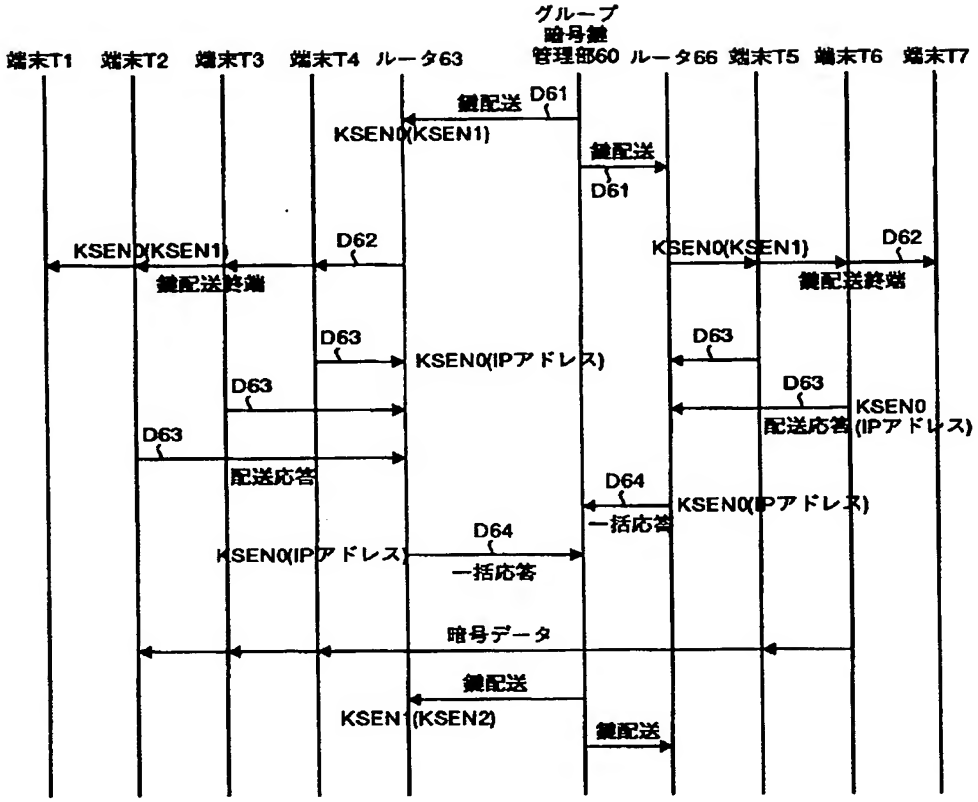
【図５】


グループ
暗号鍵
管理部40
端末T1
端末T2
端末T3
端末T4
ルータ42
ルータ44
端末T5
端末T6
端末T7
鍵配送
D1
KCC(KSE)
鍵配送
D1
D2
KCC(KSE)
鍵配送終端
D2
KCC(KSE)
鍵配送終端
D5
KP42(IP(T4))
配送応答
D5
KP44(IP(T5))
配送応答
D5
KP42(IP(T3))
配送応答
D5
KP44(IP(T6))
配送応答
D5
KP42(IP(T2))
配送応答
D6
KP40(IPアドレス)
一括応答
D6
KP40(IPアドレス)
一括応答
暗号データ

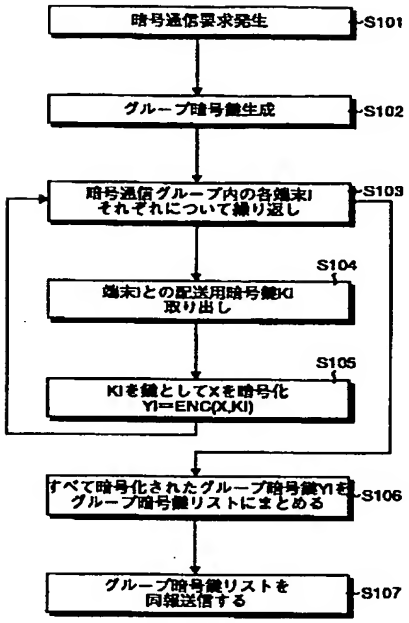
【図６】


グループ暗号鍵管理部
60
鍵配送部
61
グループ端末管理部
62
D61
D64
ネットワーク
4
ルータ
63
アドレス付加部
64
一括応答部
65
ルータ
66
アドレス付加部
67
一括応答部
68
D62
D63
D63
D63
D62
D63
D63
11
12
端末
端末
暗号鍵管理部
端末
暗号鍵管理部
端末
暗号鍵管理部
端末
暗号鍵管理部
端末
暗号鍵管理部
端末
T1
T2
t62
T3
t63
T4
t64
T5
t65
T6
t66
T7
暗号通信グループ13

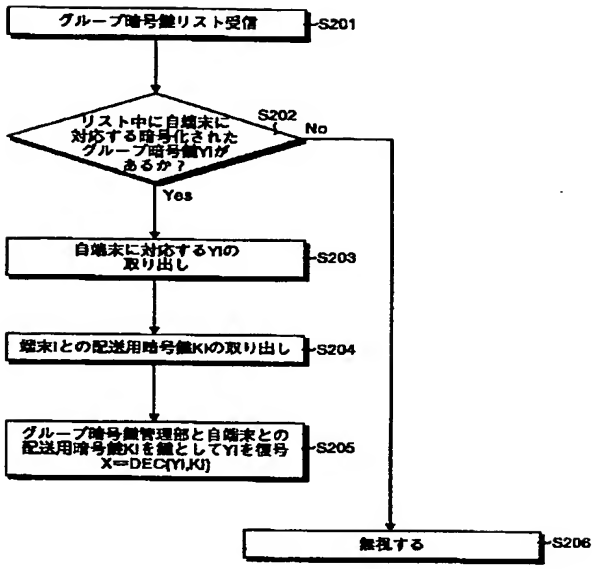
【図７】


グループ
暗号鍵
管理部60
端末T1
端末T2
端末T3
端末T4
ルータ63
ルータ66
端末T5
端末T6
端末T7
鍵配送
D61
KSEN0(KSEN1)
鍵配送
D61
KSEN0(KSEN1)
D62
KSEN0(KSEN1)
D62
鍵配送終端
鍵配送終端
D63
KSEN0(IPアドレス)
D63
D63
D63
KSEN0
配送応答
(IPアドレス)
D63
配送応答
D64
KSEN0(IPアドレス)
一括応答
D64
KSEN0(IPアドレス)
一括応答
暗号データ
鍵配送
KSEN1(KSEN2)
鍵配送

【図９】


暗号通信要求発生
S101
グループ暗号鍵生成
S102
暗号通信グループ内の各端末I
それぞれについて繰り返し
S103
S104
端末Iとの配送用暗号鍵KI
取り出し
S105
KIを鍵としてXを暗号化
YI=ENC(X,KI)
すべて暗号化されたグループ暗号鍵YIを
グループ暗号鍵リストにまとめる
S106
グループ暗号鍵リストを
同報送信する
S107

【図１０】


グループ暗号鍵リスト受信
S201
リスト中に自端末に
対応する暗号化された
グループ暗号鍵YIが
あるか？
S202
No
Yes
自端末に対応するYIの
取り出し
S203
端末Iとの配送用暗号鍵KIの取り出し
S204
グループ暗号鍵管理部と自端末との
配送用暗号鍵KIを鍵としてYIを復号
X=DEC(YI,KI)
S205
無視する
S206